PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-204320
(43)Date of publication of application : 18.07.2003

(51)Int.Cl. H04L 9/08

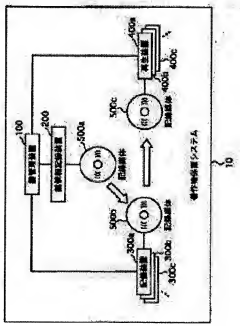
(21)Application number : 2002-303509
(22)Date of filing : 17.10.2002

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : NAKANO TOSHIHISA
MATSUZAKI NATSUME
TATEBAYASHI MAKOTO

(30)Priority
Priority number : 2001329863 Priority date : 26.10.2001 Priority country : JP

(54) LITERARY WORK PROTECTING SYSTEM, KEY MANAGEMENT SYSTEM, AND USER PROTECTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a key management system for determining an allotted key effectively and provide a recording unit, a reproducing unit, and a recording medium.
SOLUTION: In a system made up of a recording unit for recording digital data of contents like a movie or a reproducing unit, and a recording medium, a media key used for recording or reproduction is enciphered by a plurality of device keys and stored in the recording medium. In the key management system, an arrangement, in which each node-annihilation pattern allotted to a node of a tree structure is arranged in a given regulation, is stored as header information along with an enciphered medium key in the recording medium. In the recording unit or the reproducing unit, an enciphered media key to be decoded by itself is specified from the plurality of enciphered media keys by analyzing the node-annihilation pattern sequentially.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－204320
（P2003－204320Ａ）
(43)公開日　平成15年７月18日（2003.7.18）

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ04Ｌ　9/08		Ｈ04Ｌ　9/00	601Ｂ	5Ｊ104
			601Ａ	

審査請求　未請求　請求項の数26　ＯＬ　（全 51 頁）

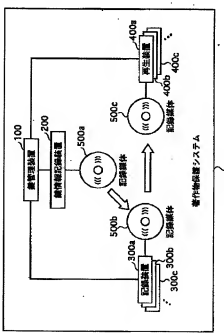
(21)出願番号　特願2002－303509(P2002－303509)
(22)出願日　平成14年10月17日(2002.10.17)
(31)優先権主張番号　特願2001－329863(P2001－329863)
(32)優先日　平成13年10月26日(2001.10.26)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　中野　稔久
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　松崎　なつめ
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100090446
弁理士　中島　司朗

最終頁に続く

(54)【発明の名称】　著作物保護システム、鍵管理装置及び利用者装置

(57)【要約】
【課題】　割り当てられた鍵を効率良く決定する鍵管理装置、記録装置、再生装置、記録媒体を提供する。
【解決手段】　映画などのコンテンツをデジタル化したデータを記録する記録装置又は再生する再生装置と、記録媒体とからなるシステムにおいて、記録媒体には、記録又は再生に使用するメディア鍵が、複数のデバイス鍵により暗号化されて記録されている。鍵管理装置は、木構造のノードに割り当てたノード無効化パターンを、ある規則に従って並べたものを鍵情報のヘッダ情報として、暗号化されたメディア鍵と共に記録媒体に記録する。記録装置又は再生装置は、ノード無効化パターンをシーケンシャルに解析することで、自身が復号すべき暗号化されたメディア鍵を複数の暗号化されたメディア鍵の中から特定する。



1

【特許請求の範囲】

【請求項１】　ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置と、１以上の利用者装置とからなる著作物保護システムであって、前記鍵管理装置は、デバイス鍵を各利用者装置に割り当て、各利用者装置は、割り当てられたデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号し、

前記鍵管理装置は、

ｎ分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、

複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、

リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段とを備え、

前記利用者装置は、

前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、

特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、

生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段とを備えることを特徴とする著作物保護システム。

【請求項２】　ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当てる鍵管理装置であって、

ｎ分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上

2

のデバイス鍵を記憶しているデバイス鍵記憶手段と、

複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、

リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段とを備えることを特徴とする鍵管理装置。

【請求項３】　前記ｎ分木は、複数のレイヤから構成され、

前記鍵情報生成手段は、得られた複数の暗号化メディア鍵を、ルートを起点とし、ルート側のレイヤからリーフ側のレイヤへの順序である前記配列順序に従って記録媒体に書き込み、

前記無効化情報生成手段は、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込むことを特徴とする請求項２に記載の鍵管理装置。

【請求項４】　前記鍵情報生成手段は、得られた複数の暗号化メディア鍵を、ルートを起点とし、ルートから各リーフへ至る経路上に配される各ノードの順序であって、重複して配列されない前記配列順序に従って記録媒体に書き込み、

前記無効化情報生成手段は、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込むことを特徴とする請求項２に記載の鍵管理装置。

【請求項５】　前記無効化情報生成手段は、リーフを除き、無効化された全てのノードについて、無効化情報を生成することを特徴とする請求項２に記載の鍵管理装置。

【請求項６】　前記無効化情報生成手段は、

リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す特別無効化情報を生成し、

前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成を抑制し、

リーフを除く他の無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成することを特徴とする請求項２に記載の鍵管理装置。

【請求項７】　前記無効化情報生成手段は、

リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについ

て、下位側に接続する全てのノードが無効化されている旨を示す第１付加情報と、下位のｎ個のノードのそれぞれが無効化されていることを示すｎ桁の情報とから構成される特別無効化情報を生成し、

前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成を抑制し、

リーフを除く他の無効化されたノードについて、下位側に接続する全てのノードが無効化されていない旨を示す第２付加情報と、下位のｎ個のノードのそれぞれが無効化されているか否かを示すｎ桁の情報とから構成される無効化情報を生成することを特徴とする請求項６に記載の鍵管理装置。

【請求項８】　前記無効化情報生成手段は、

リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位のｎ個のノードのそれぞれが無効化されていることを示すｎ桁の特別値から構成される特別無効化情報を生成し、

前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成を抑制し、

リーフを除く他の無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示すｎ桁の無効化情報を生成することを特徴とする請求項６に記載の鍵管理装置。

【請求項９】　ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当てる鍵管理装置であって、

ｎ分木において一部のノードは、無効化されており、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、

複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、

リーフを除き、無効化された各ノードについて、

下位のｎ個のノードの少なくとも１個が無効化されている場合に、それぞれが無効化されているか否かを示す第１無効化情報を生成し、

下位のｎ個のノードのいずれも無効化されていない場合に、いずれのノードも無効化されていないことを示す第２無効化情報を生成し、

その結果、１個以上の第１無効化情報、１個以上の第２無効化情報、又は１個以上の第１無効化情報及び１個以上の第２無効化情報が得られ、

得られた１個以上の第１無効化情報、１個以上の第２無効化情報、又は１個以上の第１無効化情報及び１個以上の第２無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段とを備えることを特徴とする鍵管理装置。

【請求項１０】　ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当てる鍵管理装置であって、

ｎ分木を構成する全てのノードは、有効であり、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、

各利用者装置に共通に割り当てられた１個のデバイス鍵に基づいて、１個のメディア鍵を暗号化して１個の暗号化メディア鍵を生成し、生成した前記暗号化メディア鍵を、記録媒体に書き込む鍵情報生成手段と、

ｎ分木を構成する全てのノードが有効であることを示す情報を前記記録媒体に書き込む無効化情報生成手段とを備えることを特徴とする鍵管理装置。

【請求項１１】　ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１個以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置であって、

前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、

前記利用者装置は、

前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、

特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を

生成する復号手段と、
生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段とを備えることを特徴とする利用者装置。

【請求項１２】　前記ｎ分木は、複数のレイヤから構成され、
前記複数の暗号化メディア鍵は、ルートを起点とし、ルート側のレイヤからリーフ側のレイヤへの順序である前記配列順序に従って記録媒体に書き込まれ、
前記複数の無効化情報は、前記配列順序に従って前記記録媒体に書き込まれ、
前記特定手段は、前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、前記暗号化メディア鍵を特定することを特徴とする請求項１１に記載の利用者装置。

【請求項１３】　前記複数の暗号化メディア鍵は、ルートを起点とし、ルートから各リーフへ至る経路上に配されるノードの順序であって、重複して配列されない前記配列順序に従って記録媒体に書き込まれ、
前記複数の無効化情報は、前記配列順序に従って前記記録媒体に書き込まれ、前記特定手段は、前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、前記暗号化メディア鍵を特定することを特徴とする請求項１１に記載の利用者装置。

【請求項１４】　リーフを除き、無効化された全てのノードについて、無効化情報が生成されて、前記記録媒体に書き込まれ、
前記特定手段は、前記複数の無効化情報を用いて、前記暗号化メディア鍵を特定することを特徴とする請求項１１に記載の利用者装置。

【請求項１５】　リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す特別無効化情報が生成されて前記記録媒体に書き込まれ、
前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成が抑制され、
リーフを除く他の無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報が生成されて前記記録媒体に書き込まれ、
前記特定手段は、前記特別無効化情報及び前記無効化情報を用いて、前記暗号化メディア鍵を特定することを特徴とする請求項１１に記載の利用者装置。

【請求項１６】　リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す第１付加情報と、下位のｎ個のノードのそれぞれが無効化されているか否かを示すｎ桁の情報とから構成される特別無効化情報が生成されて前記記録媒体に書き込まれ、
前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成が抑制され、
リーフを除く他の無効化されたノードについて、下位側に接続する全てのノードが無効化されていない旨を示す第２付加情報と、下位のｎ個のノードのそれぞれが無効化されているか否かを示すｎ桁の情報とから構成される無効化情報が生成されて前記記録媒体に書き込まれ、
前記特定手段は、前記特別無効化情報及び前記無効化情報を用いて、前記暗号化メディア鍵を特定することを特徴とする請求項１５に記載の利用者装置。

【請求項１７】　リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位のｎ個のノードのそれぞれが無効化されていることを示すｎ桁の特別値から構成される特別無効化情報が生成されて前記記録媒体に書き込まれ、
前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成が抑制され、
リーフを除く他の無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示すｎ桁の無効化情報が生成されて前記記録媒体に書き込まれ、
前記特定手段は、前記特別無効化情報及び前記無効化情報を用いて、前記暗号化メディア鍵を特定することを特徴とする請求項１５に記載の利用者装置。

【請求項１８】　ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１個以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置であって、
前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、一部のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化された各ノードについて、下位のｎ個のノードの少なくとも１個が無効化されている場合に、それぞれが無効化されているか否かを示

す第１無効化情報を生成し、下位のｎ個のノードのいずれも無効化されていない場合に、いずれのノードも無効化されていないことを示す第２無効化情報を生成し、その結果、１個以上の第１無効化情報、１個以上の第２無効化情報、又は１個以上の第１無効化情報及び１個以上の第２無効化情報、ｌ個以上の第２無効化情報、又は１個以上の第１無効化情報及び１個以上の第２無効化情報を、前記配列順序に従って前記記録媒体に書き込み、

前記利用者装置は、

前記記録媒体に前記配列順序に従って書き込まれた前記第１無効化情報、前記第２無効化情報、又は前記第１無効化情報及び前記第２無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、

特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、

生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段とを備えることを特徴とする利用者装置。

【請求項１９】　ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１個以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置であって、

前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ｎ分木を構成する全てのノードは、有効であり、各利用者装置に共通に割り当てられた１個のデバイス鍵に基づいて、１個のメディア鍵を暗号化して１個の暗号化メディア鍵を生成し、生成した前記暗号化メディア鍵を、記録媒体に書き込み、ｎ分木を構成する全てのノードが有効であることを示す情報を前記記録媒体に書き込み、

前記利用者装置は、

前記記録媒体に有効であることを示す前記情報が記録されていると判断する場合に、前記記録媒体に記録されている前記暗号化メディア鍵を読み出す読出手段と、

読み出した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、

生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段とを備えることを特徴とする利用者装置。

【請求項２０】　ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置で用いられる鍵管理プログラムであって、前記鍵管理装置は、ｎ分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、前記デバイス鍵を各利用者装置に割り当て、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段を備え、

前記鍵管理プログラムは、

複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成ステップと、

リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成ステップとを含むことを特徴とする鍵管理プログラム。

【請求項２１】　ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置で用いられる利用者プログラムであって、

前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従っ

て前記記録媒体に書き込み、
前記利用者プログラムは、
前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定ステップと、
特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号ステップと、
生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号ステップとを含むことを特徴とする利用者プログラム。
【請求項２２】　ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置で用いられる鍵管理方法であって、前記鍵管理装置は、ｎ分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、前記デバイス鍵を各利用者装置に割り当て、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段を備え、
前記鍵管理方法は、
無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵をそれぞれ用いて、１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成ステップと、
リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成ステップとをを含むことを特徴とする鍵管理方法。
【請求項２３】　ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１以上のデバイス鍵が割り当てられ、割り当てられた複数のデバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置で用いられる利用方法であって、
前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、
リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、
前記利用方法は、
前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定ステップと、
特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号ステップと、
生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号ステップとを含むことを特徴とする利用方法。
【請求項２４】　ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置で用いられる鍵管理プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、前記鍵管理装置は、ｎ分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、前記デバイス鍵を各利用者装置に割り当て、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段を備え、
前記鍵管理プログラムは、
複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成ステップと、
リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従っ

て前記記録媒体に書き込む無効化情報生成ステップとを含むことを特徴とする記録媒体。

【請求項２５】　ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１以上のデバイス鍵が割り当てられ、割り当てられた複数のデバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置で用いられる利用者プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、

前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、

前記利用者プログラムは、

前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定ステップと、

特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号ステップと、

生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号ステップとを含むことを特徴とする記録媒体。

【請求項２６】　コンピュータ読み取り可能な記録媒体であって、

ｎ分木（ｎは、２以上の整数）の構成に係る配列順序に従って、複数の暗号化メディア鍵及び複数の無効化情報を記録しており、

ここで、前記複数の暗号化メディア鍵及び前記複数の無効化情報は、鍵管理装置により生成され、記録され、前記鍵管理装置は、ｎ分木に関連付けて１個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当て、前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込むことを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、デジタル著作物を記録媒体に記録し、記録媒体を配布し、配布された記録媒体からデジタル著作物を再生する技術に関し、特に、著作権を保護するためのコンテンツ暗号化のための鍵情報を管理する技術に関する。

【０００２】

【従来の技術】近年、デジタル処理、蓄積、通信等の技術の発展に伴い、映画などのデジタルコンテンツを格納している大容量記録媒体を販売又はレンタルによりユーザに提供するサービスが普及している。また、デジタル化されたコンテンツが放送され、受信装置がデジタルコンテンツを受信し、受信したデジタルコンテンツを記録型デジタル光ディスク等の記録媒体に格納し、再生装置が記録媒体に格納されたデジタルコンテンツを再生するというシステムも普及しつつある。

【０００３】こうしたサービスやシステムが提供される際には、コンテンツが不正に使用されないように、コンテンツの著作権が保護され、著作権者との合意による制限の下でのみコンテンツの再生や複製などが行われる必要がある。一般的には、次に示すようにして、著作物を著作権者の許可のない不正コピー等から保護する。記録装置がデジタルコンテンツをある暗号化鍵により暗号化し、暗号化コンテンツをディスクに記録する。前記暗号化鍵に対応する復号鍵を持つ再生装置だけが暗号化コンテンツを復号できる。記録装置や再生装置などの製造業者と著作権者との間で著作権保護に対する規定が取り決められ、その規定の遵守を条件として、製造業者は、暗号化鍵又は復号鍵（以降、これらを単に、鍵と称する。）を入手できる。製造業者は、入手した鍵が外部に露見しないように厳重に管理しなければならない。

【０００４】しかし、製造業者が鍵を厳重に管理したと

しても、不正な第三者（以下、不正者）が、何らかの手段により鍵を取得することがあるかもしれない。こうして鍵が一旦不正者により暴露されてしまうと、この不正者は、製造業者と著作権者との合意による規定を逸れて、鍵自体を流布したり、コンテンツを不正に扱う記録装置又は再生装置を製造したり、又はコンテンツを不正に扱うコンピュータプログラムを作成しインターネット等を介して流布することが考えられる。このような場合、著作権者は、一旦暴露された鍵では、次から提供するコンテンツを扱えないようにしたいと考える。

【０００５】著作権者のこのような要求に答えるための最も単純な方法を次に示す。鍵管理機関は、複数のデバイス鍵及び複数のメディア鍵からなる集合を有している。鍵管理機関は、複数の記録装置及び複数の再生装置のそれぞれに、１個のデバイス鍵及びそのデバイス鍵の鍵識別番号を割り当て、割り当てたデバイス鍵及び鍵識別番号を記録装置又は再生装置に与える。また、記録媒体に、１個のメディア鍵を割り当てる。次に、鍵管理機関は、前記記録装置及び前記再生装置のそれぞれに割り当てられた各デバイス鍵を用いてメディア鍵を暗号化して暗号化メディア鍵を作成し、全てのデバイス鍵に対する暗号化メディア鍵と鍵識別番号からなるリストを鍵情報として記録媒体に格納する。記録媒体が装着された記録装置又は再生装置は、自らに割り当てられた鍵識別番号に対応する暗号化メディア鍵を、前記記録媒体の鍵情報から取り出し、自らに割り当てられたデバイス鍵を用いて、取り出した暗号化メディア鍵を復号してメディア鍵を獲得する。次に、記録装置は、獲得したメディア鍵を用いてコンテンツを暗号化して記録媒体に記録する。一方、再生装置は、同様にして獲得したメディア鍵を用いて暗号化コンテンツを復号する。このようにして、正規にデバイス鍵が割り当てられた記録装置又は再生装置であれば、１個の記録媒体からは必ず同じメディア鍵が獲得できるので、機器間の互換性が保たれる。

【０００６】ここで、ある記録装置又は再生装置のデバイス鍵が暴露されたと想定する。デバイス鍵が暴露された後、鍵管理機関が鍵情報を新たな記録媒体に格納するときに、鍵管理機関は、暴露されたデバイス鍵を除いて鍵情報を作成し、記録媒体に格納する。このようにすると、暴露されたデバイス鍵を知っている不正な装置は、記録媒体に格納されている鍵情報に、暴露されたデバイス鍵を用いて暗号化された暗号化メディア鍵が含まれていないので、鍵情報から正しいメディア鍵を獲得することができない。この結果、不正な装置は、コンテンツの不正な使用をすることができない。例えば、その不正な装置が記録装置であれば、その記録装置で記録した暗号化コンテンツは、正しいメディア鍵を用いて暗号化されていないので、他の正規の再生装置では復号することができない。また、その不正な装置が再生装置であれば、正しいメディア鍵を獲得することができないので、他の正規の記録装置で記録された暗号化コンテンツを正しく復号することができない。このようにして、暴露された鍵を無効化することができる。

【０００７】しかし、この単純な方法では、装置の台数が大量になると鍵情報のデータサイズが非現実的な大きな値になるという欠点がある。例えば、あるデジタル機器が世界的に普及し、全世界で１０億台の機器が存在するものとする。また、上述した暗号化コンテンツの生成に用いる暗号アルゴリズムとして、米国の標準暗号であるトリプルＤＥＳ暗号を用いるものとすると、メディア鍵の長さは、パディングも含めて、１６［Ｂ（バイト）］となる。従って暗号化メディア鍵の長さも１６［Ｂ］となる。さらに鍵識別番号として４［Ｂ］の値を持つとすると、全体の鍵情報サイズは２０［Ｂ］×１０億台＝２００億［Ｂ］＝２０［ＧＢ］となる。これは現在の記録型光ディスクの容量からすると非現実的な大きな値である。

【０００８】そこで、このようなシステムは、記録媒体に記録する鍵情報サイズが記録媒体の記録容量に比べわずかである、という条件を満たすものでなければならない。このような条件を満たすシステムの一例として、文献（１）「デジタルコンテンツ保護用鍵管理方式」（中野、大森、館林、2001年暗号と情報セキュリティシンポジウム、SCIS2001 5A-5, Jan. 2001）には、木構造を用いた著作権保護用鍵管理方式が開示されている。

【０００９】

【特許文献１】「デジタルコンテンツ保護用鍵管理方式」（中野、大森、館林、2001年暗号と情報セキュリティシンポジウム、SCIS2001 5A-5, Jan. 2001）ここで、文献（１）において開示されている方式について説明する前に、木構造について若干の解説を行う。形式的に、木構造は、１個以上のノードを要素とする有限集合Ｔであって、次の条件を満たすものとして定義される。

【００１０】（ａ）木構造のルートと呼ばれるノードが、１個だけ指定されている。

（ｂ）ルートを除く他のノードは、ｍ個（ｍ≧０）の共通部分を持たない集合Ｔ１、・・・、Ｔｍ に分割され、各Ｔｉ（ｉ＝１、・・・、ｍ）は再び木構造であり、これらは、Ｔよりも高さが「１」だけ小さい部分木である。この木構造Ｔ１、・・・、Ｔｍ を、そのルートに対する部分木という。

【００１１】また、木構造Ｔにおける水準（＝レイヤ）とは、次のように定義された数である。Ｔのルートの水準は０である。このルートに対する部分木をＴｊ とする場合、Ｔｊ に含まれるノードのＴにおける水準は、Ｔｊ における水準より１だけ大きい。以下では、文献（１）により開示されている木構造を用いた著作権保護用鍵管理方式について説明する。

【００１２】前記著作権保護用鍵管理方式において、鍵管理機関は、一例として、レイヤ数４の２分木である木

構造を構築し、構築した木構造に含まれるノードと同じ数のデバイス鍵を生成し、生成したデバイス鍵を構築した前記木構造の各ノードに割り当てる。鍵管理機関は、木構造の各リーフに各プレーヤ（以降、上述の再生装置と同義で使用）を対応させ、リーフからルートに至るまでの経路上に割り当てられた複数のデバイス鍵を１個のデバイス鍵セットとして、各リーフに１対１で対応するプレーヤに対して、配布する。こうして各プレーヤに配布されたデバイス鍵セットは、プレーヤごとに全て異なる。

【００１３】ここで、１個のプレーヤに割り当てられたデバイス鍵セットが暴露された場合において、鍵管理機関は、木構造において、暴露されたデバイス鍵セットに含まれるデバイス鍵が割り当てられているノードを削除する。次に、デバイス鍵が暴露されていないプレーヤの中で、最も多くのプレーヤが共有しているデバイス鍵を、次に使うべきデバイス鍵とする。

【００１４】この方式によれば、１０僧台の装置のうち、任意の１万台を無効化するためには、概ね３［ＭＢ］程度の鍵情報サイズでよいことが文献（１）に示されている。また、文献（２）「Manipulation of Trees in Information Retrieval」（G.Salton、Communication of the ACM 5、1962）及び文献（３）「基本算法／情報構造」（米田、篤訳、サイエンス社、昭53）は、木構造を１次元で表現する表現方法を開示している。木構造の各ノードをある規則に従って並べることで、木構造は１次元で表現される。例えば、文献（３）のｐ．１３６には、水準順の並べ方が示されている。これによると、水準については小さい方から大きい方へ順に並べ、それぞれの水準については、その水準内の各ノードを左から右への順に従って並べる。このような特定の規則に基づく並べ方を利用することにより、プレーヤ側で、１次元に並べた情報から木構造を構築することができる。

【００１５】

【特許文献２】「Manipulation of Trees in Information Retrieval」（G. Salton、Communication of the ACM 5、1962）

【００１６】

【特許文献３】「基本算法／情報構造」（米田、篤訳、サイエンス社、昭53）

【００１７】

【発明が解決しようとする課題】上述の著作権保護用鍵管理方式では、記録媒体に記録する鍵情報サイズが記録媒体の記録容量に比べわずかであるという条件を満たすものの、木構造により構築された鍵において、無効化されたものを含む場合に、プレーヤにおいて自らに割り当てられた鍵を効率良く決定することが要求されている。そこで本発明は、前記の要求に対処するために、利用者が有する利用者装置において、割り当てられた鍵を効率良く決定することができる著作物保護システム、鍵管理装置、利用者装置、鍵管理方法、鍵管理プログラム及び鍵管理プログラムを記録している記録媒体を提供することを目的とする。

【００１８】

【課題を解決するための手段】上記目的を達成するために、本発明は、ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置と、１以上の利用者装置とからなる著作物保護システムであって、前記鍵管理装置は、デバイス鍵を各利用者装置に割り当て、各利用者装置は、割り当てられたデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号し、前記鍵管理装置は、ｎ分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段とを備え、前記利用者装置は、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段とを備えることを特徴とする。

【００１９】また、本発明は、ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当てる鍵管理装置であって、ｎ分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段

と、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段とを備えることを特徴とする。

【００２０】ここで、前記ｎ分木は、複数のレイヤから構成され、前記鍵情報生成手段は、得られた複数の暗号化メディア鍵を、ルートを起点とし、ルート側のレイヤからリーフ側のレイヤへの順序である前記配列順序に従って記録媒体に書き込み、前記無効化情報生成手段は、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込むように構成してもよい。

【００２１】ここで、前記鍵情報生成手段は、得られた複数の暗号化メディア鍵を、ルートを起点とし、ルートから各リーフへ至る経路上に配されるノードの順序であって、重複して配列されない前記配列順序に従って記録媒体に書き込み、前記無効化情報生成手段は、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込むように構成してもよい。

【００２２】ここで、前記無効化情報生成手段は、リーフを除き、無効化された全てのノードについて、無効化情報を生成するように構成してもよい。ここで、前記無効化情報生成手段は、リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す特別無効化情報を生成し、前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成を抑制し、リーフを除く他の無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成するように構成してもよい。

【００２３】ここで、前記無効化情報生成手段は、リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す第１付加情報と、下位のｎ個のノードのそれぞれが無効化されていることを示すｎ桁の情報とから構成される特別無効化情報を生成し、前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成を抑制し、リーフを除く他の無効化されたノードについて、下位側に接続する全てのノードが無効化されていない旨を示す第２付加情報と、下位のｎ個のノードのそれぞれが無効化されているか否かを示すｎ桁の情報とから構成される無効化情報を生成するように構成してもよい。

【００２４】ここで、前記無効化情報生成手段は、リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位のｎ個のノードのそれぞれが無効化されていることを示すｎ桁の特別値から構成される特別無効化情報を生成し、前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成を抑制し、リーフを除く他の無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示すｎ桁の無効化情報を生成するように構成してもよい。

【００２５】また、本発明は、ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当てる鍵管理装置であって、ｎ分木において一部のノードは、無効化されており、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、リーフを除き、無効化された各ノードについて、下位のｎ個のノードの少なくとも１個が無効化されている場合に、それぞれが無効化されているか否かを示す第１無効化情報を生成し、下位のｎ個のノードのいずれも無効化されていない場合に、いずれのノードも無効化されていないことを示す第２無効化情報を生成し、その結果、１個以上の第１無効化情報、１個以上の第２無効化情報、又は１個以上の第１無効化情報及び１個以上の第２無効化情報が得られ、得られた１個以上の第１無効化情報、１個以上の第２無効化情報、又は１個以上の第１無効化情報及び１個以上の第２無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段とを備えることを特徴とする。

【００２６】また、本発明は、ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当てる鍵管理装置であって、ｎ分木を構成する全てのノードは、有効であり、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、各利用者装置に共通に割り当てられた１個のデバイス鍵に基づいて、１個のメディア鍵を暗号化して１個の暗号化メディア鍵を生成し、生成した前記暗号化メディア鍵を、記録媒体に書き込む鍵情報生成手段と、ｎ分

木を構成する全てのノードが有効であることを示す情報を前記記録媒体に書き込む無効化情報生成手段とを備えることを特徴とする。

【００２７】また、本発明は、ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１個以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置であって、前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、前記利用者装置は、前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段とを備えることを特徴とする。

【００２８】ここで、前記ｎ分木は、複数のレイヤから構成され、前記複数の暗号化メディア鍵は、ルートを起点とし、ルート側のレイヤからリーフ側のレイヤへの順序である前記配列順序に従って記録媒体に書き込まれ、前記複数の無効化情報は、前記配列順序に従って前記記録媒体に書き込まれ、前記特定手段は、前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、前記暗号化メディア鍵を特定するように構成してもよい。

【００２９】ここで、前記複数の暗号化メディア鍵は、ルートを起点とし、ルートから各リーフへ至る経路上に配されるノードの順序であって、重複して配列されない前記配列順序に従って記録媒体に書き込まれ、前記複数の無効化情報は、前記配列順序に従って前記記録媒体に書き込まれ、前記特定手段は、前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、前記暗号化メディア鍵を特定するように構成してもよい。

【００３０】ここで、リーフを除き、無効化された全てのノードについて、無効化情報が生成されて、前記記録媒体に書き込まれ、前記特定手段は、前記複数の無効化情報を用いて、前記暗号化メディア鍵を特定するように構成してもよい。ここで、リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す特別無効化情報が生成されて前記記録媒体に書き込まれ、前記下位側に接続する全ての無効化されたノードについて、前記無効化情報の生成が抑制され、リーフを除く他の無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報が生成されて前記記録媒体に書き込まれ、前記特定手段は、前記特別無効化情報及び前記無効化情報を用いて、前記暗号化メディア鍵を特定するように構成してもよい。

【００３１】ここで、リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す第１付加情報と、下位のｎ個のノードのそれぞれが無効化されていることを示すｎ桁の情報とから構成される特別無効化情報が生成されて前記記録媒体に書き込まれ、前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成が抑制され、リーフを除く他の無効化されたノードについて、下位側に接続する全てのノードが無効化されていない旨を示す第２付加情報と、下位のｎ個のノードのそれぞれが無効化されているか否かを示すｎ桁の情報とから構成される無効化情報が生成されて前記記録媒体に書き込まれ、前記特定手段は、前記特別無効化情報及び前記無効化情報を用いて、前記暗号化メディア鍵を特定するように構成してもよい。

【００３２】ここで、リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位のｎ個のノードのそれぞれが無効化されていることを示すｎ桁の特別値から構成される特別無効化情報が生成されて前記記録媒体に書き込まれ、前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成が抑制され、リーフを除く他の無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示すｎ桁の無効化情報が生成されて前記記録媒体に書き込まれ、前記特

定手段は、前記特別無効化情報及び前記無効化情報を用いて、前記暗号化メディア鍵を特定するように構成してもよい。

【００３３】また、本発明は、ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１個以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置であって、前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、一部のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化された各ノードについて、下位のｎ個のノードの少なくとも１個が無効化されている場合に、それぞれが無効化されているか否かを示す第１無効化情報を生成し、下位のｎ個のノードのいずれも無効化されていない場合に、いずれのノードも無効化されていないことを示す第２無効化情報を生成し、その結果、１個以上の第１無効化情報、１個以上の第２無効化情報、又は１個以上の第１無効化情報及び１個以上の第２無効化情報が得られ、得られた１個以上の第１無効化情報、１個以上の第２無効化情報、又は１個以上の第１無効化情報及び１個以上の第２無効化情報を、前記配列順序に従って前記記録媒体に書き込み、前記利用者装置は、前記記録媒体に前記配列順序に従って書き込まれた前記第１無効化情報、前記第２無効化情報、又は前記第１無効化情報及び前記第２無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記復数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段とを備えることを特徴とする。

【００３４】また、本発明は、ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１個以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置であって、前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ｎ分木を構成する全てのノードは、有効であり、各利用者装置に共通に割り当てられた１個のデバイス鍵に基づいて、１個のメディア鍵を暗号化して１個の暗号化メディア鍵を生成し、生成した前記暗号化メディア鍵を、記録媒体に書き込み、ｎ分木を構成する全てのノードが有効であることを示す情報を前記記録媒体に書き込み、前記利用者装置は、前記記録媒体に有効であることを示す情報が記録されていると判断する場合に、前記記録媒体に記録されている前記暗号化メディア鍵を読み出す読出手段と、読み出した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段とを備えることを特徴とする。

【００３５】

【発明の実施の形態】１．第１の実施の形態

本発明に係る１の実施の形態としての著作物保護システム１０について説明する。

１．１　著作物保護システム１０の構成

著作物保護システム１０は、図１に示すように、鍵管理装置１００、鍵情報記録装置２００、記録装置３００ａ、３００ｂ、３００ｃ、・・・及び再生装置４００ａ、４００ｂ、４００ｃ、・・・から構成されている。

【００３６】鍵管理装置１００は、鍵情報記録装置２００により、ＤＶＤ－ＲＡＭ等のレコーダブルメディアであって、今だ何らの情報も記録されていない記録媒体５００ａに鍵情報を記録して、鍵情報が記録された記録媒体５００ｂを予め生成しておく。また、鍵管理装置１００は、記録装置３００ａ、３００ｂ、３００ｃ、・・・及び再生装置４００ａ、４００ｂ、４００ｃ、・・・のそれぞれに対して鍵情報を復号するためのデバイス鍵を割り当て、割り当てられたデバイス鍵と、デバイス鍵を識別するデバイス鍵識別情報と、記録装置３００ａ、３００ｂ、３００ｃ、・・・及び再生装置４００ａ、４００ｂ、４００ｃ、・・・を識別するＩＤ情報とを、記録装置３００ａ、３００ｂ、３００ｃ、・・・及び再生装置４００ａ、４００ｂ、４００ｃ、・・・のそれぞれに予め配布しておく。

【００３７】記録装置３００ａは、それぞれ、デジタル化されたコンテンツを暗号化して、暗号化コンテンツを生成し、生成した暗号化コンテンツを記録媒体５００ｂに記録して、記録媒体５００ｃを生成する。再生装置４

００ａは、記録媒体５００ｃから暗号化コンテンツを取り出し、取り出した暗号化コンテンツを復号して、元のコンテンツを得る。記録装置３００ｂ、３００ｃ、・・・は、記録装置３００ａと同様に動作し、再生装置４００ｂ、４００ｃ、・・・は、再生装置４００ａと同様に動作する。

【００３８】なお、以下において、記録装置３００ｂ、３００ｃ、・・・及び再生装置４００ｂ、４００ｃ、・・・をユーザ装置と呼ぶことがある。

１．１．１　鍵管理装置１００

鍵管理装置１００は、図２に示すように、木構造構築部１０１、木構造格納部１０２、デバイス鍵副当部１０３、無効化装置指定部１０４、木構造更新部１０５、鍵情報ヘッダ生成部１０６及び鍵情報生成部１０７から構成されている。

【００３９】鍵管理装置１００は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記ＲＡＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、鍵管理装置１００は、その機能を達成する。

【００４０】（１）木構造格納部１０２

木構造格納部１０２は、具体的にはハードディスクユニットから構成されており、図３に一例として示すように、木構造テーブルＤ１００を有している。木構造テーブルＤ１００は、図４に一例として示す木構造Ｔ１００に対応しており、木構造Ｔ１００を表現するためのデータ構造を示す。後述するように、木構造構築部１０１により木構造Ｔ１００を表現するためのデータ構造が、木構造テーブルＤ１００として生成され、木構造格納部１０２に書き込まれる。

【００４１】（木構造Ｔ１００）木構造Ｔ１００は、図４に示すように、レイヤ０からレイヤ４までの５階層からなる２分木である。木構造Ｔ１００は、２分木であるので、木構造Ｔ１００が有する各ノード（リーフを除く）は、２本の経路を介して下位側の２個のノードにそれぞれ接続されている。レイヤ０にはルートである１個のノードが含まれ、レイヤ１には２個のノードが含まれ、レイヤ２には４個のノードが含まれ、レイヤ３には８個のノードが含まれ、レイヤ４にはリーフである１６個のノードが含まれている。なお、木構造において下位側とはリーフ側を示し、上位側とはルート側を示している。

【００４２】木構造Ｔ１００が有する各ノード（リーフを除く）と、下位側のノードとを接続する２本の経路のうち、一方である左の経路には、「０」の番号が割り当てられており、他方である右の経路には「１」の番号が割り当てられている。ここで、図４の紙面において、各ノードを中心として当該ノードから左側下方に接続されている経路を左の経路と称し、当該ノードから右側下方に接続されている経路を右の経路と称している。

【００４３】各ノードには、ノード名が付されている。ルートであるノードのノード名は、「ルート」である。また、レイヤ１を含め、レイヤ１より下位にあるレイヤに属するノードに対しては、レイヤ数が示す値と同じ文字数からなる文字列がノード名として付されている。この文字列は、ルートから当該ノードに至るまでの経路に割り当てられた番号を、上位から順に並べて生成されたものである。例えば、レイヤ１に属する２個のノードのノード名は、それぞれ「０」及び「１」である。また、レイヤ２に属する４個のノードのノード名は、それぞれ「００」、「０１」、「１０」及び「１１」である。また、レイヤ３に属する８個のノードのノード名は、それぞれ「０００」、「００１」、「０１０」、「０１１」、・・・、「１０１」、「１１０」及び「１１１」である。また、レイヤ４に属する１６個のノードのノード名は、それぞれ「００００」、「０００１」、「０００１」、「０００１」、「０１１０」、「０１１１」、・・・、「１１００」、「１１０１」、「１１１０」及び「１１１１」である。

【００４４】（木構造テーブルＤ１００）木構造テーブルＤ１００は、木構造Ｔ１００に含まれるノードと同じ数のノード情報を含んで構成されており、各ノード情報は、木構造Ｔ１００を構成する各ノードにそれぞれ対応している。各ノード情報は、ノード名、デバイス鍵及び無効化フラグを含む。

【００４５】ノード名は、当該ノード情報に対応するノードを識別するための名称である。デバイス鍵は、当該ノード情報に対応するノードに対して割り当てられた鍵である。また、当該ノード情報に対応するデバイス鍵が無効化されているか否かを示すフラグであり、無効化フラグが「０」である場合には、無効化されていないことを示し、無効化フラグが「１」である場合には、無効化されていることを示す。

【００４６】木構造テーブルＤ１００内には、次に示す順序規則１に従った順序により各ノード情報が記憶される。ここに示す順序規則１は、記録装置３００ａ、３００ｂ、３００ｃ、・・・、再生装置４００ａ、４００ｂ、４００ｃ、・・・により、木構造テーブルＤ１００から各ノード情報がシーケンシャルに読み出される場合においても適用される。

【００４７】（ａ）木構造テーブルＤ１００内には、木構造Ｔ１００のレイヤ数の昇順に、各レイヤに属するノードに対応するノード情報が記憶される。具体的には、木構造テーブルＤ１００内には、最初にレイヤ０に属する１個のルートに対応する１個のノード情報が記憶され、次に、レイヤ１に属する２個のノードに対応する２個のノード情報が記憶され、次に、レイヤ２に属する４個のノードに対応する４個のノード情報が記憶される。

以下同様である。

【００４８】（ｂ）各レイヤに属するノードについては、各ノードを識別するノード名の昇順により、対応するノード情報が記憶される。具体的には、図３に示す木構造テーブルＤ１００内には、次に示す順序により各ノード情報が記憶される。「ルート」、「０」、「１」、「００」、「０１」、「１０」、「１１」、「０００」、「０００１」、「００１０」、「００１１」、・・・、「０１０」、「０１１０」、「０１１１」、「１０００」、「１０００１」、「１０００１０」、「１０００１１」、・・・、「１１００」、「１１０１」、「１１１０」、「１１１１」ここでは、各ノード情報に含まれるノード名により、各ノード情報が記憶されている順序を示している。

【００４９】（２）木構造構築部１０１

木構造構築部１０１は、以下に示すようにして、デバイス鍵を管理するためのｎ分木のデータ構造を構築し、木構造格納部１０２に構築した木構造を格納する。ここで、ｎは２以上の整数であり、一例として、ｎ＝２である。木構造構築部１０１は、最初に、ノード名として「ルート」を含むノード情報を生成し、木構造格納部１０２が有している木構造テーブルへ書き込む。

【００５０】次に、木構造構築部１０１は、レイヤ１について、２個のノードを識別するノード名「０」及び「１」を生成し、生成したノード名「０」及び「１」をそれぞれ含む２個のノード情報を生成し、生成した２個のノード情報をこの順序で、木構造格納部１０２が有している木構造テーブルへ追加して書き込む。次に、木構造構築部１０１は、レイヤ２について、４個のノードを識別するノード名「００」、「０１」、「１０」及び「１１」を生成し、生成したノード名「００」、「０１」、「１０」及び「１１」をそれぞれ含む４個のノード情報を生成し、生成した４個のノード情報をこの順序で、木構造格納部１０２が有している木構造テーブルへ追加して書き込む。

【００５１】以降、木構造構築部１０１は、レイヤ３及びレイヤ４について、この順序で、上記と同様にして、ノード情報の生成と、木構造テーブルへの書き込みとを行う。木構造構築部１０１は、次に、木構造のノード毎に乱数を用いてデバイス鍵を生成し、生成したデバイス鍵を各ノードに対応付けて木構造テーブル内に書き込む。

【００５２】（３）デバイス鍵割当部１０３

デバイス鍵割当部１０３は、以下に示すようにして、木構造格納部１０２に格納されている木構造から、ユーザ装置が割り当てられていないリーフと、デバイス鍵を与えるべきユーザ装置を対応付けて適当なデバイス鍵を選択し、選択したデバイス鍵をユーザ装置へ出力する。

【００５３】デバイス鍵割当部１０３は、４ビット長の変数ＩＤを有している。デバイス鍵割当部１０３は、以下に示す処理（ａ）～（ｆ）を１６回繰り返す。１６回の繰り返しのそれぞれにおいて、変数１Ｄは、「００００」、「０００１」、「００１０」、・・・、「１１１０」、「１１１１」の値を保持する。１６回の繰り返しにより、デバイス鍵割当部１０３は、１６台のユーザ装置のそれぞれにＩＤ情報と５個のデバイス鍵とを割り当てる。

【００５４】（ａ）デバイス鍵割当部１０３は、木構造格納部１０２が有する木構造テーブルから、「ルート」のノード名を含むノード情報を取得し、取得したノード情報に含まれるデバイス鍵を抽出する。抽出したデバイス鍵が、ルートに割り当てられたデバイス鍵である。

（ｂ）デバイス鍵割当部１０３は、木構造格納部１０２が有する木構造テーブルから、変数１Ｄの先頭１ビットからなるノード名を含むノード情報を取得し、取得したノード情報に含まれるデバイス鍵を抽出する。ここで、抽出したデバイス鍵をデバイス鍵Ａとする。

【００５５】（ｃ）デバイス鍵割当部１０３は、木構造格納部１０２が有する木構造テーブルから、変数ＩＤの先頭２ビットからなるノード名を含むノード情報を取得し、取得したノード情報に含まれるデバイス鍵を抽出する。ここで、抽出したデバイス鍵をデバイス鍵Ｂとする。

（ｄ）デバイス鍵割当部１０３は、木構造格納部１０２が有する木構造テーブルから、変数１Ｄの先頭３ビットからなるノード名を含むノード情報を取得し、取得したノード情報に含まれるデバイス鍵を抽出する。ここで、抽出したデバイス鍵をデバイス鍵Ｃとする。

【００５６】（ｅ）デバイス鍵割当部１０３は、木構造格納部１０２が有する木構造テーブルから、変数ＩＤの先頭４ビットからなるノード名を含むノード情報を取得し、取得したノード情報に含まれるデバイス鍵を抽出する。ここで、抽出したデバイス鍵をデバイス鍵Ｄとする。

（ｆ）デバイス鍵割当部１０３は、ＩＤ情報としての変数ＩＤ、ルートに割り当てられたデバイス鍵、各ノードに割り当てられたデバイス鍵Ａ、Ｂ、Ｃ、Ｄ、、及び前記５個のデバイス鍵をそれぞれ識別する５個のデバイス鍵識別情報を、ユーザ装置が有する鍵情報記憶部へ書き込む。

【００５７】こうして、各ユーザ装置の鍵情報記憶部は、図８に一例として示すように、ＩＤ情報、５個のデバイス鍵識別情報及び５個のデバイス鍵を記憶する。ここで、５個のデバイス鍵識別情報と５個のデバイス鍵とは、それぞれ対応付けられている。各デバイス鍵識別情報は、対応するデバイス鍵が割り当てられているノードが属するレイアの数（レイア数）である。

【００５８】以上のようにして、１６台のユーザ装置のそれぞれに、１Ｄ情報及び５個のデバイス鍵が割り当てられる。一例として、図４に示す木構造Ｔ１００は、上述したように、レイヤ数５の２分木であり、１６個のリ

ーフを含んでいる。ここで、ユーザ装置は、１６台あるものとし、１６台のユーザ装置は、各々１６個のリーフに対応している。各ユーザ装置には、木構造Ｔ１００において、対応するリーフからルートに至るまでの経路上に位置するノードに割り当てられたデバイス鍵がそれぞれ与えられる。例えば、ユーザ装置１には、ＩＫ１、ＫｅｙＨ、ＫｅｙＤ、ＫｅｙＢ、ＫｅｙＡの５つのデバイス鍵が与えられる。また、例えば、ユーザ装置１には、ＩＤ情報「０００Ｄ」が与えられ、ユーザ装置１４には、ＩＤ情報「１１０１」が与えられる。

【００５９】（４）無効化装置指定部１０４

無効化装置指定部１０４は、鍵管理装置１００の運営管理者から、無効化する１台以上のユーザ装置をそれぞれ識別する１個以上のＩＤ情報を受け付け、受け付けたＩＤ情報を木構造更新部１０５へ出力する。

（５）木構造更新部１０５

木構造更新部１０５は、無効化装置指定部１０４から１個以上のＩＤ情報を受け取る。ＩＤ情報を受け取ると、受け取った１個以上のＩＤ情報のそれぞれについて、次に示す処理（ａ）～（ｄ）を繰り返す。

【００６０】（ａ）木構造更新部１０５は、受け取ったＩＤ情報をノード名として含むノード情報を木構造格納部１０２が有する木構造テーブルから取得し、取得したノード情報に無効化フラグ「１」を付加し、無効化フラグ「１」が付加されたノード情報を、木構造テーブル上において、取得した前記ノード情報が記憶されていた位置に上書きする。

【００６１】（ｂ）木構造更新部１０５は、受け取ったＩＤ情報の先頭３ビットをノード名として含むノード情報を木構造格納部１０２が有する木構造テーブルから取得し、上記と同様にして、取得したノード情報に無効化フラグ「１」を付加して木構造テーブルに上書きする。

（ｃ）木構造更新部１０５は、受け取ったＩＤ情報の先頭２ビットをノード名として含むノード情報を木構造格納部１０２が有する木構造テーブルから取得し、上記と同様にして、取得したノード情報に無効化フラグ「１」を付加して木構造テーブルに上書きする。

【００６２】（ｄ）木構造更新部１０５は、「ルート」をノード名として含むノード情報を木構造格納部１０２が有する木構造テーブルから取得し、上記と同様にして、取得したノード情報に無効化フラグ「１」を付加して木構造テーブルに上書きする。

以上説明したように、木構造更新部１０５は、無効化装置指定部１０４から受け取ったＩＤ情報に基づいて、木構造において、受け取ったＩＤ情報が示すリーフから、ノードまでの経路上に存在する全てのノードを無効化する。

【００６３】図４に示す木構造Ｔ１００において、ＩＤ情報「００００」、「１０１０」及び「１０１１」により示されるユーザ装置が無効化されると想定する場合、上記のようにしてノードが無効化された木構造Ｔ２００を図５に示す。また、木構造テーブルＤ１００は、木構造Ｔ２００に対応して無効化フラグが付加されたものである。

【００６４】木構造Ｔ２００において、ＩＤ情報「００００」により示されるユーザ装置１に対応するリーフからルートまでの経路に存在する全てのノード、ＩＤ情報「１０１０」により示されるユーザ装置１１に対応するリーフからルートまでの経路に存在する全てのノード、及びＩＤ情報「１０１１」により示されるユーザ装置１２に対応するリーフからルートまでの経路に存在する全てのノードに、×印が付されているが、これらのノードは、無効化されたノードを示している。

【００６５】木構造テーブルＤ１００において、上記の無効化されたノードに対応するノード情報には、無効化フラグが付加されている。

（６）鍵情報ヘッダ生成部１０６

鍵情報ヘッダ生成部１０６は、レイヤ数を示す変数ｉ及びレイヤに含まれるノード名を示す変数ｊを有している。

【００６６】鍵情報ヘッダ生成部１０６は、次に示す処理（ａ）を、木構造に含まれるレイヤ数分、繰り返す。レイヤ数分の繰り返しのそれぞれにおいて、レイヤ数を示す変数ｉは、「０」、「１」、「２」、「３」の値を保持する。

（ａ）鍵情報ヘッダ生成部１０６は、変数ｉによりレイヤ数が示されるレイヤに含まれる全てのノードの数だけ、ノード毎に次に示す処理（ａ－１）～（ａ－３）を繰り返す。ここで、処理（ａ－１）～（ａ－３）の対象となる対象ノード名を変数ｊにより示す。

【００６７】（ａ－１）鍵情報ヘッダ生成部１０６は、木構造格納部１０２が有する木構造テーブルから、変数ｊに「０」を結合して得られるノード名を含むノード情報を取得し、変数ｊに「１」を結合して得られるノード名を含むノード情報を取得する。このようにして得られた２個のノード情報は、それぞれ、変数ｊにより示される対象ノードの直下に接続されている２個の下位ノードに対応している。

【００６８】（ａ－２）鍵情報ヘッダ生成部１０６は、取得した２個の前記ノード情報のそれぞれに含まれている無効化フラグの両方が「０」であるか、否かを調べ、両方が「０」でない場合に、取得した２個の前記ノード情報のそれぞれに含まれている２個の無効化フラグを、２個の前記ノード情報が木構造テーブルに格納されている順序で並べて、ノード無効化パターン（Ｎｏｄｅ　ＲｅｖｏｃａｔｉｏｎＰａｔｔｅｒｎ、以下、ＮＲＰと呼ぶ。）を生成する。

【００６９】具体的には、取得した２個の前記ノード情報のそれぞれに含まれている無効化フラグが「０」及び「０」である場合には、ノード無効化パターンを生成し

ない。また、取得した２個の前記ノード情報のそれぞれに含まれている無効化フラグが「１」及び「０」である場合には、ＮＲＰ｛１０｝を生成する。

【００７０】取得した２個の前記ノード情報のそれぞれに含まれている無効化フラグが「０」及び「１」である場合には、ＮＲＰ｛０１｝を生成する。取得した２個の前記ノード情報のそれぞれに含まれている無効化フラグが「１」及び「１」である場合には、ＮＲＰ｛１１｝を生成する。（ａ－３）鍵情報ヘッダ生成部１０６は、生成したＮＲＰを鍵情報記録装置２００へ出力する。

【００７１】以上説明したように、鍵情報ヘッダ生成部１０６は、木構造のレイヤ内のノード毎に、当該ノードの下位側に直接接続されている２個の下位ノードが無効化されているか否かを調べ、２個の下位ノードのいずれか一方が無効化されている場合には、上記に示すようにしてＮＲＰを生成する。図５に示す木構造Ｔ２００において、×印が付されたノードの近辺に、当該ノードに対応して生成したＮＲＰを示している。

【００７２】また、鍵情報ヘッダ生成部１０６は、上記に示すような繰り返しにおいて、ＮＲＰを出力するので、図５に示す場合には、図６に一例として示す複数個のＮＲＰが生成されて出力される。鍵情報ヘッダ生成部１０６は、これらの複数個のＮＲＰをヘッダ情報として出力する。図５に示す木構造Ｔ２００において、ユーザ装置１、ユーザ装置１１及びユーザ装置１２がそれぞれ無効化されている。ここで、無効化されるべき各ユーザ装置に対応するリーフから、ルートに至るまでの経路上に存在するノード（図５において、×印が付されたノード）を無効化ノードと称する。また、１個のノードの子ノードが無効化ノードである場合を「１」、そうでない場合を「０」で表現し、それら子ノードの状態を左から順に連結したものが、そのノードのＮＲＰである。ＮＲＰは、ｎ分木の場合、ｎビットの情報である。図５における木構造Ｔ２００のルートＴ２０１について、２つの子ノードが共に無効化ノードであるため、ＮＲＰは、｛１１｝と表現される。また、ノードＴ２０２に付されたＮＲＰは、｛１０｝と表現される。また、ノードＴ２０３は、無効化ノードであるが、子ノードが存在しないリーフであるため、ＮＲＰは付加されない。

【００７３】図６に一例として示すように、ヘッダ情報Ｄ２００は、ＮＲＰ｛１１｝、｛１０｝、｛１０｝、｛１０｝、｛０１｝、｛１０｝、｛１１｝から構成され、各ＮＲＰをこの順序で含んでいる。なお、これらの複数個のＮＲＰのそれぞれは、ヘッダ情報Ｄ２００内において格納される位置が定められている。この位置は、上記の繰り返しにより定まるものである。図６に示すように、ヘッダ情報Ｄ２００内に「０」、「１」、「２」、「３」、「４」、「５」及び「６」により定まる位置において、それぞれ、ＮＲＰ｛１１｝、｛１０｝、｛１０｝、｛０１｝、｛１０｝、｛１１｝が配置されている。

【００７４】以上説明したように、鍵情報ヘッダ生成部１０６は、無効化ノードの１以上のＮＲＰを抽出し、抽出したＮＲＰを鍵情報のヘッダ情報として、鍵情報記録装置２００へ出力する。このとき、鍵情報ヘッダ生成部１０６は、複数のＮＲＰを水準順に並べる。すなわち、複数のＮＲＰを上位レイヤから下位レイヤの順に並べ、レイヤが同じＮＲＰついては、左から右への順に並べる。なお、ＮＲＰの並べ方はある規則に基づいていればよく、例えば、レイヤが同じ場合に右から左の順に並べるとしてもよい。

【００７５】（７）鍵情報生成部１０７

鍵情報生成部１０７は、鍵情報ヘッダ生成部１０６と同様に、レイヤ数を示す変数ｉ及びレイヤに含まれるノード名を示す変数ｊを有している。鍵情報生成部１０７は、次に示す処理（ａ）を、木構造に含まれ、レイヤ０を除くレイヤ数分、繰り返す。レイヤ数分の繰り返しのそれぞれにおいて、レイヤ数を示す変数ｉは、「１」、「２」、「３」の値を保持する。

【００７６】（ａ）鍵情報生成部１０７は、変数ｉによりレイヤ数が示されるレイヤに含まれる全てのノードの数だけ、ノード毎に次に示す処理（ａ－１）～（ａ－３）を繰り返す。ここで、処理（ａ－１）～（ａ－３）の対象となる対象ノード名を変数ｊにより示す。

（ａ－１）鍵情報生成部１０７は、木構造格納部１０２が有する木構造テーブルから、変数ｊをノード名として含むノード情報を取得し、取得したノード情報に含まれる無効化フラグが「１」であるか又は「０」であるかを判断する。

【００７７】（ａ－２）無効化フラグが「０」である場合に、鍵情報生成部１０７は、さらに、対象ノードの上位に接続されている上位ノードに対応するデバイス鍵による暗号化がされているか否かを判断する。

（ａ－３）暗号化がされていない場合に、鍵情報生成部１０７は、取得したノード情報に含まれるデバイス鍵を抽出し、暗号化アルゴリズムＥ１を適用して、抽出したデバイス鍵を用いて、生成されたメディア鍵を暗号化して、暗号化メディア鍵を生成する。

【００７８】暗号化メディア鍵＝Ｅ１（デバイス鍵、メディア鍵）

ここで、Ｅ（Ａ、Ｂ）は、暗号化アルゴリズムＥを適用して、鍵Ａを用いて、データＢを暗号化することを示している。また、暗号化アルゴリズムＥ１は、一例として、ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）である。

【００７９】次に、鍵情報生成部１０７は、生成した暗号化メディア鍵を鍵情報記録装置２００へ出力する。なお、無効化フラグ「１」が付されている場合、又は暗号化がされている場合には、処理（ａ－３）は、行われない。以上説明したように、鍵情報生成部１０７は、上記

に示すような繰り返しにおいて、暗号化メディア鍵を出力するので、図５に示す場合には、図７に一例として示す複数個の暗号化メディア鍵が生成されて出力される。鍵情報生成部１０７は、これらの複数個の暗号化メディア鍵を鍵情報Ｄ３００として出力する。

【００８０】なお、これらの複数個の暗号化メディア鍵のそれぞれは、鍵情報Ｄ３００内において格納されている位置が定められている。この位置は、上記の繰り返しにより定まるものである。図７に示すように、鍵情報Ｄ３００内に「０」、「１」、「２」、「３」及び「４」により定まる位置において、それぞれ、暗号化メディア鍵Ｅ１（ＫｅｙＥ、メディア鍵）、Ｅ１（ＫｅｙＧ、メディア鍵）、Ｅ１（ＫｅｙＩ、メディア鍵）、Ｅ１（ＫｅｙＬ、メディア鍵）、Ｅ１（ＩＫ２、メディア鍵）が配置されている。

【００８１】１．１．２　鍵情報記録装置２００

鍵情報記録装置２００は、鍵情報ヘッダ生成部１０６から鍵情報を受け取り、鍵情報生成部１０７から鍵情報を受け取り、受け取ったヘッダ情報と鍵情報とを記録媒体５００ａに書き込む。

１．１．３　記録媒体５００ａ、ｂ、ｃ

記録媒体５００ａは、ＤＶＤ－ＲＡＭ等のレコーダブルメディアであって、今だ何らの情報も記録されていないものである。

【００８２】記録媒体５００ｂは、記録媒体５００ａに、鍵管理装置１００及び鍵情報記録装置２００により、上記に述べたようにして、ヘッダ情報が付加された鍵情報が書き込まれたものである。記録媒体５００ｃは、記録媒体５００ｂに、記録装置３００ａ、３００ｂ、３００ｃ、・・・の何れかにより、上記に述べたようにして、暗号化コンテンツがが書き込まれたものである。

【００８３】図８に示すように、記録媒体５００ｃは、ヘッダ情報が付加された鍵情報と暗号化コンテンツとを記録している。

１．１．４　記録装置３００ａ、３００ｂ、３００ｃ、・・・

記録装置３００ａは、図８に示すように、鍵情報記憶部３０１、復号部３０２、特定部３０３、暗号部３０４及びコンテンツ記憶部３０５から構成されている。なお、記録装置３００ｂ、３００ｃ、・・・は、記録装置３００ａと同様の構成を有しているので、これらについて説明を省略する。

【００８４】記録装置３００ａは、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどを含んで構成され、前記ＲＡＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、記録装置３００ａは、その機能を達成する。記録装置３００ａには、記録媒体５００ｂが装着される。記録装置３００ａは、自らが記憶しているＩＤ情報を元に記録媒体５００ｂに記憶されているヘッダ情報の解析を行って、復号すべき暗号化メディア鍵の位置と、使用すべきデバイス鍵を特定し、特定したデバイス鍵を用いて復号してメディア鍵を獲得する。次に、獲得したメディア鍵を用いて、デジタル化されたコンテンツを暗号化し、暗号化コンテンツを記録媒体５００ｂに記録する。

【００８５】（１）鍵情報記憶部３０１

鍵情報記憶部３０１は、ＩＤ情報と、５個のデバイス鍵と、５個のデバイス鍵識別情報とを記憶するための５個のデバイス鍵識別情報とを記憶するための領域を備えている。

（２）特定部３０３

特定部３０３は、鍵管理装置１００が有する鍵情報ヘッダ生成部１０６が、鍵情報のヘッダ情報を上述した順序規則１に従って生成したものと想定して動作する。

【００８６】特定部３０３は、鍵情報記憶部３０１からＩＤ情報を読み出す。また、記録媒体５００ｂからヘッダ情報及び鍵情報を読み出す。次に、特定部３０３は、読み出したＩＤ情報及び読み出したヘッダ情報を用いて、ヘッダ情報を上位からシーケンシャルに調べていくことにより、鍵情報の中から１個の暗号化メディア鍵が存在する位置Ｘと、前記暗号化メディア鍵の復号に使用するデバイス鍵を識別するためのデータ鍵識別情報とを特定する。なお、暗号化メディア鍵が存在する位置Ｘ及びデバイス鍵識別情報を特定する場合の詳細の動作については、後述する。

【００８７】次に、特定部３０３は、特定した１個の暗号化メディア鍵及び決定した１個のデバイス鍵識別情報を復号部３０２へ出力する。

（３）復号部３０２

復号部３０２は、特定部３０３から１個の暗号化メディア鍵及び１個のデバイス鍵識別情報を受け取る。１個の暗号化メディア鍵及び１個のデバイス鍵識別情報を受け取ると、受け取ったデバイス鍵識別情報により識別されるデバイス鍵を鍵情報記憶部３０１から読み出し、復号アルゴリズムＤ１を適用して、読み出したデバイス鍵を用いて、受け取った暗号化メディア鍵を復号して、メディア鍵を生成する。

【００８８】メディア鍵＝Ｄ１（デバイス鍵、暗号化メディア鍵）

ここで、Ｄ（Ａ、Ｂ）は、復号アルゴリズムＤを適用して、鍵Ａを用いて、暗号化データＢを復号して元のデータを生成することを意味する。また、復号アルゴリズムＤ１は、暗号化アルゴリズムＥ１に対応するものであり、暗号化アルゴリズムＥ１を適用して暗号化されたデータを復号するためのアルゴリズムである。

【００８９】次に、復号部３０２は、生成したメディア鍵を暗号部３０４へ出力する。なお、図８に記載されている各ブロックは、接続線により他のブロックと接続さ

れている。ただし、一部の接続線を省略している。ここで、各接続線は、信号や情報が伝達される経路を示している。また、復号部３０２を示すブロックに接続している複数の接続線のうち、接続線上に鍵マークが付されているものは、復号部３０２へ鍵としての情報が伝達される経路を示している。暗号部３０４を示すブロックについても同様である。また、他の図面についても同様である。

【００９０】（４）コンテンツ記憶部３０５

コンテンツ記憶部３０５は、デジタル化された音楽などの著作物であるコンテンツを記憶している。

（５）暗号部３０４

暗号部３０４は、復号部３０２からメディア鍵を受け取り、コンテンツ記憶部３０５からコンテンツを読み出す。次に、暗号部３０４は、暗号化アルゴリズムＥ２を適用して、受け取ったメディア鍵を用いて、読み出したコンテンツを暗号化して暗号化コンテンツを生成する。

【００９１】暗号化コンテンツ＝Ｅ２（メディア鍵、コンテンツ）

ここで、暗号化アルゴリズムＥ２は、一例として、ＤＥＳによる暗号化アルゴリズムである。次に、暗号部３０４は、生成した暗号化コンテンツを記録媒体５００ｂへ書き込む。このようにして、暗号化コンテンツが書き込まれた記録媒体５００ｃが生成される。

【００９２】１．１．５　再生装置４００ａ、４００ｂ、４００ｃ、・・・

再生装置４００ａは、図９に示すように、鍵情報記憶部４０１、特定部４０２、復号部４０３、復号部４０４及び再生部４０５から構成されている。なお、再生装置４００ｂ、４００ｃ、・・・は、再生装置４００ａと同様の構成を有しているので、これらについて説明を省略する。

【００９３】再生装置４００ａは、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどを含んで構成され、前記ＲＡＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、再生装置４００ａは、その機能を達成する。ここで、鍵情報記憶部４０１、特定部４０２及び復号部４０３は、それぞれ、記録装置３００ａが有している鍵情報記憶部３０１、特定部３０３及び復号部３０２と同様の構成を有しているので、説明を省略する。

【００９４】再生装置４００ａに記録媒体５００ｃが装着される。再生装置４００ａは、自ら記憶しているＩＤ情報を元に、記録媒体５００ｃに記憶されているヘッダ情報の解析を行って、復号すべき暗号化メディア鍵の位置と、使用すべきデバイス鍵を特定し、特定したデバイス鍵を用いて復号してメディア鍵を獲得する。次に、再生装置４００ａは、獲得したメディア鍵を用いて、記録媒体５００ｃに記録されている暗号化コンテンツを復号してコンテンツを再生する

（１）復号部４０４

復号部４０４は、復号部４０３からメディア鍵を受け取り、記録媒体５００ｃから暗号化コンテンツを読み出し、復号アルゴリズムＤ２を適用して、受け取ったメディア鍵を用いて、読み出した前記暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツを再生部４０５へ出力する。

【００９５】コンテンツ＝Ｄ２（メディア鍵、暗号化コンテンツ）

ここで、復号アルゴリズムＤ２は、暗号化アルゴリズムＥ２に対応するものであり、暗号化アルゴリズムＥ２を適用して暗号化されたデータを復号するためのアルゴリズムである。

（２）再生部４０５

再生部４０５は、復号部４０４からコンテンツを受け取り、受け取ったコンテンツを再生する。例えば、コンテンツが音楽の場合には、再生部４０５は、コンテンツを音声に変換して出力する。

【００９６】１．２．著作物保護システム１０の動作

著作物保護システム１０の動作について説明する。

１．２．１　デバイス鍵の割り当て、記録媒体の生成及びコンテンツの暗号化又は復号の動作

ここでは、ユーザ装置へデバイス鍵を割り当てる動作、鍵情報の生成と記録媒体への書き込みの動作及びユーザ装置によるコンテンツの暗号化又は復号の動作について、図１０に示すフローチャートを用いて説明する。特に、デバイス鍵が不正な第三者により暴露されるまでの、各装置の動作について説明する。

【００９７】鍵管理装置１００の木構造構築部１０１は、木構造を表す木構造テーブルを生成し、生成した木構造テーブルを木構造格納部１０２へ書き込み（ステップＳ１０１）、次に、木構造のノード毎にデバイス鍵を生成し、生成したデバイス鍵を各ノードに対応付けて木構造テーブル内に書き込む（ステップＳ１０２）。次に、デバイス鍵割当部１０３は、デバイス鍵、デバイス鍵識別情報及びＩＤ情報を対応するユーザ装置へ出力する（ステップＳ１０３～Ｓ１０４）。ユーザ装置が有する鍵情報記憶部は、デバイス鍵、デバイス鍵識別情報及びＩＤ情報を受け取り（ステップＳ１０４）、受け取ったデバイス鍵、デバイス鍵識別情報及びＩＤ情報を記録する（ステップＳ１１１）。

【００９８】このようにして、デバイス鍵、デバイス鍵識別情報及びＩＤ情報を記録しているユーザ装置が生産され、生産されたユーザ装置がユーザに対して販売される。次に、鍵情報生成部１０７は、メディア鍵を生成し（ステップＳ１０５）、鍵情報を生成し（ステップＳ１０６）、生成した鍵情報を鍵情報記録装置２００を介して記録媒体５００ａに出力し（ステップＳ１０７～Ｓ１０８）、記録媒体５００ａは、鍵情報を記録する（ステ

ップＳ１２１）。

【００９９】このようにして、鍵情報が記録された記録媒体５００ｂが生成され、生成された記録媒体５００ｂが販売などされることにより、利用者に配布される。次に、鍵情報が記録された記録媒体が、ユーザ装置に装着され、ユーザ装置は、記録媒体から鍵情報を読み出し（ステップＳ１３１）、読み出した鍵情報を用いて、当該ユーザ装置自身に割り当てられた暗号化メディア鍵を特定し（ステップＳ１３２）、メディア鍵を復号し（ステップＳ１３３）、復号したメディア鍵を用いて、コンテンツを暗号化して記録媒体５００ｂに書き込み、又は暗号化コンテンツの記録されている記録媒体５００ｃから暗号化コンテンツを読み出し、読み出した暗号化コンテンツを復号したメディア鍵を用いて復号して、コンテンツを生成する（ステップＳ１３４）。

【０１００】以上のように、ユーザ装置により暗号化コンテンツを記録媒体５００ｂに書き込み、ユーザ装置により暗号化コンテンツの記録されている記録媒体５００ｃから暗号化コンテンツを読み出して復号し、コンテンツを再生する。次に、不正な第三者が、ユーザ装置に割り当てられたデバイス鍵を、何らかの手段により不正に取得する。不正な第三者は、前記コンテンツを不正に流通させたり、正規のユーザ装置を模倣する不正な装置を生産して販売する。

【０１０１】鍵管理装置１００の運営管理者は、又は前記コンテンツの著作権者は、コンテンツが不正に流通していること、又は不正な装置が流通していることを知り、前記デバイス鍵が漏洩したことを知る。

１．２．２　デバイス鍵が暴露された後の動作

ここでは、デバイス鍵が不正な第三者により暴露された後における、暴露されたデバイス鍵に対応する木構造の内のノードの無効化の動作、新たな鍵情報の生成と記録媒体への書込みの動作、及びユーザ装置によるコンテンツの暗号化又は復号の動作について、図１１に示すフローチャートを用いて説明する。

【０１０２】鍵管理装置１００の無効化装置指定部１０４は、無効化する１台以上のユーザ装置の１個以上のＩＤ情報を受け付け、受け付けたＩＤ情報を木構造更新部１０５へ出力する（ステップＳ１５１）。次に、木構造更新部１０５は、ＩＤ情報を受け取り、受け取ったＩＤ情報を用いて、木構造を更新し（ステップＳ１５２）、鍵情報ヘッダ生成部１０６は、ヘッダ情報を生成し、生成したヘッダ情報を鍵情報記録装置２００へ出力し（ステップＳ１５３）、鍵情報生成部は、メディア鍵を生成し（ステップＳ１５４）、鍵情報を生成し（ステップＳ１５５）、生成した鍵情報を鍵情報記録装置２００を介して出力し（ステップＳ１５６～Ｓ１５７）、記録媒体５００ａは、鍵情報を記録する（ステップＳ１６１）。

【０１０３】このようにして、新たな鍵情報が記録された記録媒体５００ｂが生成され、生成された記録媒体５００ｂが販売などされることにより、利用者に配布される。次に、新たな鍵情報が記録された記録媒体が、ユーザ装置に装着され、ユーザ装置は、記録媒体から鍵情報を読み出し（ステップＳ１７１）、読み出した鍵情報を用いて、当該ユーザ装置自身に割り当てられた暗号化メディア鍵を特定し（ステップＳ１７２）、メディア鍵を復号し（ステップＳ１７３）、復号したメディア鍵を用いて、コンテンツを暗号化して記録媒体５００ｂに書き込み、又は暗号化コンテンツの記録されている記録媒体５００ｃから暗号化コンテンツを読み出し読み出した暗号化コンテンツを復号したメディア鍵を用いて復号して、コンテンツを生成する（ステップＳ１７４）。

【０１０４】以上のように、ユーザ装置により暗号化コンテンツを記録媒体５００ｂに書き込み、又はユーザ装置により暗号化コンテンツの記録されている記録媒体５００ｃから暗号化コンテンツを読み出して復号し、コンテンツを再生する。

１．２．３　木構造を構築して格納する動作

ここでは、木構造構築部１０１による木構造テーブルの生成と木構造格納部１０２への木構造テーブルの書き込みの動作について、図１２に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図１０に示すフローチャートにおけるステップＳ１０１の詳細である。

【０１０５】木構造構築部１０１は、最初に、ノード名として「ルート」を含むノード情報を生成し、木構造格納部１０２が有している木構造テーブルへ書き込む（ステップＳ１９１）。次に、木構造構築部１０１は、レイヤｉ（ｉ＝１、２、３、４）について、次に示すステップＳ１９３～Ｓ１９４を繰り返す。

【０１０６】木構造構築部１０１は、２ｉ 個の文字列をノード名として生成し（ステップＳ１９３）、生成した２ｉ 個の文字列をノード名として含むノード情報を、順に木構造テーブルへ書き込む（ステップＳ１９４）。

１．２．４　デバイス鍵とＩＤ情報とを各ユーザ装置へ出力する動作

ここでは、デバイス鍵割当部１０３によるデバイス鍵とＩＤ情報とを各ユーザ装置へ出力する動作について、図１３に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図１０に示すフローチャートにおけるステップＳ１０３の詳細である。

【０１０７】デバイス鍵割当部１０３は、変数ＩＤを「００００」、「０００１」、「００１０」、・・・、「１１１０」、「１１１１」のように変化させ、それぞれの変数ＩＤについて、次に示すステップＳ２２２～Ｓ２２７を繰り返す。デバイス鍵割当部１０３は、ルートに割り当てられたデバイス鍵を取得し（ステップＳ２２２）、変数ＩＤの先頭１ビットをノード名とするノードに割り当てられたデバイス鍵Ａを取得し（ステップＳ２２３）、変数ＩＤの先頭２ビットをノード名とするノー

ドに割り当てられたデバイス鍵Ｂを取得し（ステップＳ２２４）、変数ＩＤの先頭３ビットをノード名とするノードに割り当てられたデバイス鍵Ｃを取得し（ステップＳ２２５）、変数ＩＤの先頭４ビットをノード名とするノードに割り当てられたデバイス鍵Ｄを取得し（ステップＳ２２６）、ＩＤ情報としての変数ＩＤ、ルートに割り当てられたデバイス鍵、各ノードに割り当てられたデバイス鍵Ａ、Ｂ、Ｃ、Ｄをユーザ装置へ出力する（ステップＳ２２７）。

【０１０８】１．２．５　木構造の更新の動作

ここでは、木構造更新部１０５による木構造の更新の動作について、図１４に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図１１に示すフローチャートにおけるステップＳ１５２の詳細である。木構造更新部１０５は、無効化装置指定部１０４から受け取った１個以上のＩＤ情報のそれぞれについて、次に示すステップＳ２４２～Ｓ２４６を繰り返す。

【０１０９】木構造更新部１０５は、受け取ったＩＤ情報をノード名として含むノード情報を取得し、取得したノード情報に無効化フラグ「１」を付加する（ステップＳ２４２）。次に、木構造更新部１０５は、受け取ったＩＤ情報の先頭３ビットをノード名として含むノード情報を取得し、取得したノード情報に無効化フラグ「１」を付加する（ステップＳ２４３）。

【０１１０】次に、木構造更新部１０５は、受け取ったＩＤ情報の先頭２ビットをノード名として含むノード情報を取得し、取得したノード情報に無効化フラグ「１」を付加する（ステップＳ２４４）。次に、木構造更新部１０５は、受け取ったＩＤ情報の先頭１ビットをノード名として含むノード情報を取得し、取得したノード情報に無効化フラグ「１」を付加する（ステップＳ２４５）。

【０１１１】次に、木構造更新部１０５は、「ルート」をノード名として含むノード情報を取得し、取得したノード情報に無効化フラグ「１」を付加する（ステップＳ２４６）。

１．２．６　ヘッダ情報の生成の動作

ここでは、鍵情報ヘッダ生成部１０６によるヘッダ情報の生成の動作について、図１５に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図１１に示すフローチャートにおけるステップＳ１５３の詳細である。

【０１１２】鍵情報ヘッダ生成部１０６は、レイヤ０からレイヤ３までの各レイヤについて、ステップＳ２６２～Ｓ２６６を繰り返す。さらに、鍵情報ヘッダ生成部１０６は、各レイヤに含まれる対象ノード毎に、ステップＳ２６３～Ｓ２６５を繰り返す。鍵情報ヘッダ生成部１０６は、当該対象ノードの直下に接続されている２個の下位ノードを選択し（ステップＳ２６３）、次に選択した２個の下位ノードのそれぞれに無効化フラグが付されているか否かを調べてＮＲＰを生成し（ステップＳ２６４）、生成したＮＲＰを出力する（ステップＳ２６５）。

【０１１３】１．２．７　鍵情報の生成の動作

ここでは、鍵情報生成部１０７による鍵情報の生成の動作について、図１６に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図１１に示すフローチャートにおけるステップＳ１５５の詳細である。鍵情報生成部１０７は、レイヤ１からレイヤ３までの各レイヤについて、ステップＳ２８２～Ｓ２８７を繰り返す。さらに、鍵情報生成部１０７は、各レイヤに含まれる対象ノード毎に、ステップＳ２８３～Ｓ２８６を繰り返す。

【０１１４】鍵情報生成部１０７は、対象ノードに無効化フラグ「１」が付されているか否かを判断する。無効化フラグ「１」が付されていない場合には（ステップＳ２８３）、さらに対象ノードの上位に接続されている上位ノードに対応するデバイス鍵による暗号化がされているか否かを判断する。暗号化がされていない場合に（ステップＳ２８４）、対象ノードに対応するデバイス鍵を木構造テーブルから取得し（ステップＳ２８５）、取得したデバイス鍵を用いて、生成されたメディア鍵を暗号化して、暗号化メディア鍵を生成し、生成した暗号化メディア鍵を出力する（ステップＳ２８６）。

【０１１５】無効化フラグ「１」が付されている場合（ステップＳ２８３）、又は暗号化がされている場合（ステップＳ２８４）、ステップＳ２８５～Ｓ２８６は行われない。

１．２．８　鍵情報の特定の動作

ここでは、記録装置３００ａが有する特定部３０３により、記録媒体５００ｂに記憶されている鍵情報から、１個の暗号化メディア鍵を特定する動作について、図１７に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図１１に示すフローチャートにおけるステップＳ１７２の詳細である。

【０１１６】また、再生装置４００ａが有する特定部４０２による動作は、特定部３０３による動作と同じであるので、説明を省略する。特定部３０３は、暗号化メディア鍵の位置を示す変数Ｘ、ユーザ装置自身に関係するＮＲＰの位置を示す変数Ａ、あるレイヤにおけるＮＲＰの数を示す変数Ｗ、及び木構造のレイヤ数を示す値Ｄを有している。ここで、ユーザ装置自身に関係するＮＲＰ（Ｎｏｄｅ　Ｒｅｖｏｃａｔｉｏｎ　Ｐａｔｔｅｒｎ、以下、ＮＲＰと呼ぶ。）とは、木構造において、ユーザ装置に割り当てられているリーフから、ルートに至るまでの経路上に存在するノードのＮＲＰを示す。

【０１１７】特定部３０３は、レイヤｉ＝０から、レイヤｉ＝Ｄ－１まで、以下の手順で解析を行う。特定部３０３は、初期値として、それぞれ変数Ａ＝０、変数Ｗ＝１、変数１＝０とする（ステップＳ３０１）。変数ｉと

値Ｄとを比較し、変数ｉが値Ｄより大きい場合（ステップＳ３０２）、このユーザ装置は、無効化されているので、次に、特定部３０３は、処理を終了する。

【０１１８】変数ｉが値Ｄより小さいか又は等しい場合（ステップＳ３０２）、特定部３０３は、Ａ番目のＮＲＰを構成する左右２ビットのうち、ＩＤ情報の上位ｉビット目の値に対応するビット位置にある値Ｂが「０」であるか、又は「１」であるかをチェックする（ステップＳ３０３）。ここで、対応するビット位置とは、図４に示すように、木構造において左の経路に「０」、右の経路に「１」が割り当てられ、これらの規則に基づいてＩＤ情報が構成されているので、ＩＤ情報の上位ｉビット目の値「０」は、Ａ番目のＮＲＰの左ビットに対応し、ｉビット目の値「１」は、Ａ番目のＮＲＰの右ビットに対応する。

【０１１９】値Ｂ＝０の場合（ステップＳ３０３）、特定部３０３は、これまでにチェックしたＮＲＰのうち、オール「１」でないＮＲＰの数をカウントし、カウントした値を、変数Ｘに代入する。こうして得られた変数Ｘが、暗号化メディア鍵の位置を示している。また、この時点の変数ｉは、デバイス鍵を識別するためのデバイス鍵識別情報である（ステップＳ３０７）。次に、特定部３０３は、処理を終了する。

【０１２０】値Ｂ＝１の場合（ステップＳ３０３）、特定部３０３は、レイヤｉに存在するＷ個の全ＮＲＰの「１」の数をカウントし、カウントした値を変数Ｗに代入する。こうして得られた変数Ｗが、次のレイヤｉ＋１に存在するＮＲＰの数を示す（ステップＳ３０４）。次に、特定部３０３は、レイアｉに存在するＮＲＰのうちの最初のＮＲＰから、対応するビット位置までのＮＲＰをカウントし、カウントした値を変数Ａに代入する。ここで、対応するビット位置の値はカウントしない。こうして得られた変数Ａが、次のレイヤｉ＋１のＮＲＰのうち、ユーザ装置自身に関係するＮＲＰの位置を示す（ステップＳ３０５）。

【０１２１】次に、特定部３０３は、変数ｉ＝ｉ＋１を演算し（ステップＳ３０６）、次にステップＳ３０２へ制御を移し、上述の処理を繰り返す。

１．２．９　鍵情報の特定の動作の具体例

一具体例として、図６及び図７に示すヘッダ情報及び鍵情報を用いて、図５に示す無効化されていないユーザ装置１４が暗号化メディア鍵を特定するまでの動作について以下に説明する。ユーザ装置１４には、ＩＤ情報「１１０１」が割り当てられ、デバイス鍵「ＫｅｙＡ」、「ＫｅｙＣ」、「ＫｅｙＧ」、「ＫｅｙＮ」及び「ＩＫ１４」が割り当てられているものとする。

【０１２２】（ステップ１）特定部３０３は、ユーザ装置１４に割り当てられたＩＤ情報「１１０１」の最上位ビットの値が「１」であるため、最初のＮＲＰ｛１１｝の右ビットをチェックする（ステップＳ３０３）。

（ステップ２）最初のＮＲＰ｛１１｝の右ビットの値が「１」であるため、特定部３０３は、解析を続ける（ステップＳ３０３で、Ｂ＝１）。

【０１２３】（ステップ３）特定部３０３は、レイヤ０に存在する１個のＮＲＰ｛１１｝の「１」の数をカウントする。そのカウントした値が「２」であるので、次のレイヤ１には２個のＮＲＰが存在することが分かる（ステップＳ３０４）。

（ステップ４）特定部３０３は、対応するビット位置までのＮＲＰの「１」の数をカウントする。ただし、対応するビット位置の値はカウントしない。そのカウントした値が「１」であるため、次のレイヤ１の対応するＮＲＰの位置は、レイア１内で、１番目である（ステップＳ３０５）。

【０１２４】（ステップ５）次に、特定部３０３は、ＩＤ情報「１１０１」の上位から２ビット目の値が「１」であるため、レイヤ１の１番目のＮＲＰ｛１０｝の右ビットをチェックする（ステップＳ３０３）。

（ステップ６）ここで、レイヤ１の１番目のＮＲＰ｛１０｝の右ビットの値が「０」であるため、特定部３０３は、解析を終了する（ステップＳ３０３で、Ｂ＝０）。

【０１２５】（ステップ７）特定部３０３は、これまでのＮＲＰのうち、オール「１」でないＮＲＰの数をカウントする。ただし、最後にチェックしたＮＲＰはカウントしない。カウントした値が「１」であるため、暗号化メディア鍵の位置は、鍵情報内において、１番目である（ステップＳ３０７）。

（ステップ８）図７に示すように、鍵情報の１番目の位置に格納されている暗号化メディア鍵は、Ｅ１（ＫｅｙＧ，メディア鍵）である。

【０１２６】ユーザ装置１４は、ＫｅｙＧを保持している。よって、ユーザ装置１４は、ＫｅｙＧを用いて暗号化メディア鍵を復号してメディア鍵を獲得することができる。

１．３　まとめ

以上説明したように、第１の実施の形態によると、記録媒体に予め記録されている鍵情報のヘッダ情報内には、複数のＮＲＰが水準順に並べられているので、鍵情報がコンパクトになる。また、プレーヤは、復号すべき暗号化メディア鍵を効率よく特定することができる。

【０１２７】２．第２の実施の形態

ここでは、第１の実施の形態の変形例としての第２の実施の形態について説明する。第１の実施の形態において、一例として図１８に示すように、無効化されるユーザ装置が木構造の中で特定のリーフに偏って発生する可能性がある。この場合、鍵管理装置１００が記録媒体に書き込む鍵情報のヘッダ情報内において、｛１１｝であるＮＲＰが多くなる。図１８に示す例では、木構造Ｔ３００の左半分のリーフは、全て無効化された装置に対応するので、鍵情報内のヘッダ情報は、１１個のＮＲＰを

含むが、そのうち８個は｛１１｝である。

【０１２８】図１８に示す例では、木構造Ｔ３００の左半分は全て無効化された装置であるので、レイヤ１のノードから下は全て無効化ノードであると表現すれば、左半分の各ノードに対応したＮＲＰをヘッダ情報として記録媒体に記録する必要がなくなる。そこで、第２の実施の形態では、無効化された装置が木構造の中で特定のリーフに集中する場合に、ヘッダ情報のデータ量を少なく抑えることができる著作物保護システム１０ｂ（図示していない）について説明する。

【０１２９】鍵管理装置１００は、第１の実施の形態において説明したように、鍵情報のヘッダ情報として、ＮＲＰを生成する。ここで、鍵管理装置１００は、ＮＲＰの先頭に１ビットを追加する。追加したビットが「１」である場合には、そのノードの子孫のノードに割り当てられたユーザ装置は全て無効化装置であることを示す。図１９において、ノードＴ４０１及びノードＴ４０２は、これらのノードの子孫のノードに割り当てられた装置が全て無効化装置ではないので、先頭ビットは「０」であり、ＮＲＰは、それぞれ、｛０１１｝、｛０１０｝と表現される。ノードＴ４０３の子孫のノードに割り当てられた装置は、全て無効化装置であるため、ＮＲＰは｛１１｝と表現される。鍵管理装置１００は、ノードＴ４０３の子孫のノードについてのＮＲＰを記録媒体に書き込まない。

【０１３０】２．１　著作物保護システム１０ｂの構成
著作物保護システム１０ｂは、著作物保護システム１０と同様の構成を有している。ここでは、著作物保護システム１０との相違点を中心として説明する。第２の実施の形態では、図１９に示すように、ユーザ装置１～ユーザ装置８及びユーザ装置１２がそれぞれ無効化されているとする。

【０１３１】２．１．１　鍵管理装置１００
著作物保護システム１０ｂの鍵管理装置１００は、第１の実施の形態において述べた鍵管理装置１００と同様の構成を有している。ここでは、その相違点を中心として説明する。

（１）木構造格納部１０２
木構造格納部１０２は、木構造テーブルＤ１００に代えて、一例として図２０に示す木構造テーブルＤ４００を有している。

【０１３２】木構造テーブルＤ４００は、図１９に一例として示す木構造Ｔ４００に対応しており、木構造Ｔ４００を表現するためのデータ構造を示す。木構造テーブルＤ４００は、木構造Ｔ４００に含まれるノードと同じ数のノード情報を含んで構成されており、各ノード情報は、木構造Ｔ４００を構成する各ノードにそれぞれ対応している。

【０１３３】各ノード情報は、ノード名、デバイス鍵、無効化フラグ及びＮＲＰを含む。ノード名、デバイス鍵及び無効化フラグについては、第１の実施の形態で説明したとおりであるので、説明を省略する。ＮＲＰは、３ビットから構成され、上位の１ビットは、上述したように、対応するノード名により示されるノードの子孫のノードに割り当てられたユーザ装置は全て無効化装置であることを示す。下位の２ビットは、第１の実施の形態で説明したＮＲＰと同じ内容のものである。

【０１３４】（２）鍵情報ヘッダ生成部１０６
鍵情報ヘッダ生成部１０６は、ＮＲＰの先頭の１ビットが「１」である場合には、そのノードの子孫のノードに割り当てられたユーザ装置は全て無効化装置であることを示すＮＲＰを生成し、生成したＮＲＰを鍵情報記録装置２００へ出力する。なお、ＮＲＰの生成の詳細については、後述する。

【０１３５】鍵情報ヘッダ生成部１０６は、一例として、図２１に示すヘッダ情報Ｄ５００を生成する。ヘッダ情報Ｄ５００は、ＮＲＰ｛０１１｝、｛１１１｝、｛０１０｝、｛００１｝及び｛００１｝から構成され、各ＮＲＰをこの順序で含んでいる。また、この図に示すように、ヘッダ情報Ｄ５００内に「０」、「１」、「２」、「３」及び「４」により定まる位置において、それぞれ、ＮＲＰ｛０１１｝、｛１１１｝、｛０１０｝、｛００１｝及び｛００１｝が配置されている。

【０１３６】（３）鍵情報生成部１０７
鍵情報生成部１０７は、一例として、図２２に示す鍵情報Ｄ６００を生成する。鍵情報Ｄ６００は、３個の暗号化メディア鍵を含んでいる。３個の暗号化メディア鍵は、それぞれデバイス鍵ＫｅｙＧ、ＫｅｙＬ、ＩＫ１１を用いてメディア鍵を暗号化したものである。

【０１３７】これらの複数個の暗号化メディア鍵のそれぞれは、鍵情報Ｄ６００内において格納されている位置が定められている。この図に示すように、鍵情報Ｄ６００内に「０」、「１」及び「２」により定まる位置において、それぞれ、暗号化メディア鍵Ｅ１（ＫｅｙＧ、メディア鍵）、Ｅ１（ＫｅｙＬ、メディア鍵）及びＥ１（ＩＫ１１、メディア鍵）が配置されている。

【０１３８】２．１．２　記録装置３００ａ
記録装置３００ａは、第１の実施の形態において述べた記録装置３００ａと同様の構成を有している。ここでは、その相違点を中心として説明する。

（１）特定部３０３
特定部３０３は、ＩＤ情報及びヘッダ情報を用いて、ヘッダ情報を上位からシーケンシャルに調べていくことにより、鍵情報の中から１個の暗号化メディア鍵が存在する位置Ｘを特定する。なお、暗号化メディア鍵が存在する位置Ｘを特定する場合の詳細の動作については、後述する。

【０１３９】２．２　著作物保護システム１０ｂの動作
著作物保護システム１０ｂの動作について、著作物保護システム１０の動作との相違点を中心として説明する。

２．２．１　ヘッダ情報の生成の動作

ここでは、鍵情報ヘッダ生成部１０６によるヘッダ情報の生成の動作について、図２３～図２６に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図１１に示すフローチャートにおけるステップＳ１５３の詳細である。

【０１４０】鍵情報ヘッダ生成部１０６は、レイヤ０からレイヤ３までの各レイヤについて、ステップＳ３２２～Ｓ３２７を繰り返す。さらに、鍵情報ヘッダ生成部１０６は、各レイヤに含まれる対象ノード毎に、ステップＳ３２３～Ｓ３２６を繰り返す。鍵情報ヘッダ生成部１０６は、当該対象ノードの直下に接続される２個の下位ノードをチェックし（ステップＳ３２３）、選択した２個の下位ノードのそれぞれに無効化フラグが付されているか否かを調べて、ＮＲＰを生成し（ステップＳ３２４）、値「０」を有する短縮ビットを生成したＮＲＰの先頭に付加し（ステップＳ３２５）、拡張ビットが付加されたＮＲＰを木構造テーブル内の当該対象ノードに対応するノード情報内に付加する（ステップＳ２３６）。

【０１４１】以上のようにして、ステップＳ３２１～Ｓ３２８の繰返しが終了すると、第１の実施の形態において説明した方法と同様に、各ノード情報内にＮＲＰが付加される。ここで、各ＮＲＰの先頭には、値「０」（１ビット）が付加されている。次に、鍵情報ヘッダ生成部１０６は、レイヤ３からレイヤ０までの各レイヤについて、ステップＳ３３０～Ｓ３３５を繰り返す。さらに、鍵情報ヘッダ生成部１０６は、各レイヤに含まれる対象ノード毎に、ステップＳ３３１～Ｓ３３４を繰り返す。

【０１４２】鍵情報ヘッダ生成部１０６は、当該対象ノードの直下に接続される２個の下位ノードを選択し（ステップＳ３３１）、選択した２個のノードの両方にそれぞれＮＲＰ｛１１１｝が付加されているか否かを調べる。ただし、選択した２個のノードがリーフである場合には、選択した２個のノードの両方に無効化フラグが付されているか否かを調べる（ステップＳ３３２）。

【０１４３】選択した２個の下位ノードの両方にそれぞれＮＲＰ｛１１１｝が付されている場合にのみ、ただし選択した２個のノードがリーフである場合には、選択した２個の下位ノードの両方に無効化フラグが付されている場合にのみ（ステップＳ３３３）、鍵情報ヘッダ生成部１０６は、当該対象ノードに付加されたＮＲＰの先頭ビットを「１」に書き換える（ステップＳ３３４）。

【０１４４】以上のようにして、ステップＳ３２９～Ｓ３３６の繰返しが終了すると、それぞれＮＲＰ｛１１１｝が付加されている２個の下位ノードに接続する上位のノードには、｛１１１｝が付加されることになる。次に、鍵情報ヘッダ生成部１０６は、レイヤ２からレイヤ０までの各レイヤについて、ステップＳ３３８～Ｓ３４３を繰り返す。さらに、鍵情報ヘッダ生成部１０６は、各レイヤに含まれる対象ノード毎に、ステップＳ３３９～Ｓ３４２を繰り返す。

【０１４５】鍵情報ヘッダ生成部１０６は、当該対象ノードの直下に接続される２個の下位ノードを選択し（ステップＳ３３９）、選択した２個の下位ノードの両方にＮＲＰ｛１１１｝が付加されているか否かを調べる（ステップＳ３４０）。選択した２個の下位ノードの両方にＮＲＰ｛１１１｝が付加されている場合にのみ（ステップＳ３４１）、鍵情報ヘッダ生成部１０６は、選択した２個の下位ノードにそれぞれ付加されたＮＲＰを木構造テーブルから削除する（ステップＳ３４２）。

【０１４６】次に、鍵情報ヘッダ生成部１０６は、木構造テーブルに記憶されているＮＲＰをルートから順に読み出して、出力する（ステップＳ３４５）。以上のようにして、ＮＲＰの先頭の１ビットが「１」である場合に、そのノードの子孫のノードに割り当てられたユーザ装置は全て無効化装置であることを示すＮＲＰが生成される。

【０１４７】２．２．２　鍵情報の特定の動作

ここでは、記録装置３００ａが有する特定部３０３により、記録媒体５００ｂに記憶されている鍵情報から、１個の暗号化メディア鍵を特定する動作について、図２７に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図１１に示すフローチャートにおけるステップＳ１７２の詳細である。

【０１４８】また、特定部３０３による１個の暗号化メディア鍵を特定する動作は、第１の実施の形態において説明した動作と同様であり、ここでは、その相違点を中心として説明する。値Ｂ＝０の場合（ステップＳ３０３）、特定部３０３は、これまでにチェックしたＮＲＰのうち、下位２ビットがオール「１」でないＮＲＰの数をカウントし、カウントした値を、変数Ｘに代入する。こうして得られた変数Ｘが、暗号化メディア鍵の位置を示している（ステップＳ３０７ａ）。次に、特定部３０３は、処理を終了する。

【０１４９】値Ｂ＝１の場合（ステップＳ３０３）、特定部３０３は、レイヤｉに存在するＷ個の全ＮＲＰの「１」の数をカウントする。ただし、ＮＲＰの最上位のビットが「１」のＮＲＰについては、カウントしない。カウントした値を変数Ｗに代入する。こうして得られた変数Ｗが、次のレイヤｉ＋１に存在するＮＲＰの数を示す。（ステップＳ３０４ａ）。

【０１５０】次に、特定部３０３は、最初のＮＲＰから数えて、対応するビット位置までのＮＲＰの「１」の数をカウントする。ただし、ＮＲＰの最上位のビットが「１」のＮＲＰについては、カウントしない。カウントした値を変数Ａに代入する。ここで、対応するビット位置の値はカウントしない。こうして得られた変数Ａが、次のレイヤｉ＋１のＮＲＰのうち、ユーザ装置自身に関係するＮＲＰの位置を示す（ステップＳ３０５ａ）。

【０１５１】２．２．３　鍵情報の特定の動作の具体例

一具体例として、図２１及び図２２に示す鍵情報を用いて、図１９に示す無効化されていないユーザ装置１０が暗号化メディア鍵を特定するまでの動作について以下に説明する。ユーザ装置１０には、ＩＤ情報「１００１」が割り当てられ、デバイス鍵「ＫｅｙＡ」、「ＫｅｙＣ」、「ＫｅｙＦ」、「ＫｅｙＬ」及び「ＩＫ１０」が割り当てられているものとする。

【０１５２】（ステップ１）特定部３０３は、ユーザ装置１０に割り当てられたＩＤ情報「１００１」の最上位ビットの値が「１」であるため、最初のＮＲＰ｛０１１｝の下位２ビットのうちの右ビットをチェックする（ステップＳ３０３）。

（ステップ２）最初のＮＲＰ｛０１１｝の下位２ビットのうちの右ビットの値が「１」であるため、特定部３０３は、解析を続ける（ステップＳ３０３で、Ｂ＝１）。

【０１５３】（ステップ３）特定部３０３は、レイヤ０に存在する１個のＮＲＰ｛０１１｝の下位２ビットのうちの「１」の数をカウントする。そのカウントした値が「２」であるため、次のレイヤ１には２個のＮＲＰが存在することが分かる（ステップＳ３０４ａ）。

（ステップ４）特定部３０３は、対応するビット位置までのＮＲＰ｛０１１｝の下位２ビットの「１」の数をカウントする。ただし、対応するビット位置の値はカウントしない。そのカウントした値が「１」であるため、次のレイヤ１の対応するＮＲＰの位置は、レイヤ１内において、１番目である（ステップＳ３０５ａ）。

【０１５４】（ステップ５）次に、特定部３０３は、ＩＤ情報「１００１」の上位から２ビット目の値が「０」であるため、レイヤ１の１番目のＮＲＰ｛０１０｝の下位２ビットのうちの左ビットをチェックする（ステップＳ３０３）。

（ステップ６）ここで、レイヤ１の１番目のＮＲＰ｛０１０｝の下位２ビットのうちの左ビットの値が「１」であるため、特定部３０３は、解析を続ける（ステップＳ３０３で、Ｂ＝１）。

【０１５５】（ステップ７）特定部３０３は、レイヤ１に存在する２個のＮＲＰ｛１１１｝、｛０１０｝の下位２ビットのうちの「１」の数をカウントする。ただし、ＮＲＰの最上位ビットが「１」であるＮＲＰについては、カウントしない。そのカウントした値が「１」であるため、次のレイヤ２には１個のＮＲＰが存在することが分かる（ステップＳ３０４ａ）。

【０１５６】（ステップ８）特定部３０３は、対応するビット位置までのＮＲＰの「１」の数をカウントする。ただし、対応するビット位置の値はカウントしない。そのカウントした値が「０」であるため、次のレイヤ２の対応するＮＲＰの位置は、レイヤ２内において、０番目である（ステップＳ３０５ａ）。

（ステップ９）次に、特定部３０３は、ＩＤ情報「１００１」の上位から３ビット目の値が「０」であるため、レイヤ２の０番目のＮＲＰ｛００１｝の下位２ビットのうちの左ビットをチェックする（ステップＳ３０３）。

【０１５７】（ステップ１０）ここで、レイヤ２の０番目のＮＲＰ｛００１｝の下位２ビットのうちの左ビットの値が「０」であるため、特定部３０３は、解析を終了する（ステップＳ３０３で、Ｂ＝０）。

（ステップ１１）特定部３０３は、これまでに解析したＮＲＰのうち、下位２ビットが、オール「１」でないＮＲＰの数をカウントする。なお、最後にチェックしたＮＲＰは、カウントしない。カウントした値が「１」であるため、暗号化メディア鍵の位置は、鍵情報内において、１番目である（ステップＳ３０７ａ）。

【０１５８】（ステップ１２）図２２より、鍵情報の１番目の位置に格納されている暗号化メディア鍵は、Ｅ１（ＫｅｙＬ，メディア鍵）である。ユーザ装置１０は、ＫｅｙＬを保持している。よって、ユーザ装置１０は、ＫｅｙＬを用いて暗号化メディア鍵を復号してメディア鍵を獲得することができる。

【０１５９】なお、上述した第２の実施の形態においては、あるノードの子孫に存在するユーザ装置が全て無効化装置である場合に、追加するビットを「１」としている。しかし、リーフのレイヤ数がそれぞれ異なるような木構造がある場合、あるノードの子孫にＮＲＰが存在しない場合は、追加したビットを「１」にすることで終端を意味するフラグとしても使用することができる。

【０１６０】３．第３の実施の形態

上記の第２の実施の形態においては、あるノードの子孫が全て無効化装置であるか否かを示すビットをＮＲＰの先頭に追加することで、無効化装置が集中した場合に、ヘッダ情報をさらに少なく抑える方法を示している。次に述べる第３の実施の形態では、ＮＲＰにビットを追加する代わりに、特定のパターン｛００｝を有するＮＲＰを用いて、１個のノードの子孫が全て無効化装置であるか否かを判断する。これは、レイヤ０を除く全てのレイヤにおいては、ＮＲＰ｛００｝が使われないことに着目したものである。これにより、第２の実施の形態よりも、さらにヘッダ情報を少なく抑えることができる著作物保護システム１０ｃ（図示していない）について説明する。ここでは、図２８に示すように、ユーザ装置１～ユーザ装置８、ユーザ装置１２がそれぞれ無効化されているとする。第３の実施の形態では、ＮＲＰは第１の実施の形態に示す通りであるが、あるノードの子孫のユーザ装置が全て無効化装置である場合には、そのノードのＮＲＰを｛００｝で表現する。図２８におけるノードＴ５０１について、そのノードの子孫が全て無効化装置であるため、ＮＲＰは｛００｝と表現されている。

【０１６１】３．１　著作物保護システム１０ｃの構成

著作物保護システム１０ｃは、著作物保護システム１０と同様の構成を有している。ここでは、著作物保護システム１０との相違点を中心として説明する。

３．１．１　鍵管理装置１００

著作物保護システム１０ｃの鍵管理装置１００は、第１の実施の形態において述べた鍵管理装置１００と同様の構成を有している。ここでは、その相違点を中心として説明する。

【０１６２】（１）鍵情報ヘッダ生成部１０６

鍵情報ヘッダ生成部１０６は、ＮＲＰが｛００｝である場合には、そのノードの子孫のノードに割り当てられたユーザ装置は全て無効化装置であることを示すＮＲＰを生成し、生成したＮＲＰを鍵情報記録装置２００へ出力する。なお、ＮＲＰの生成の詳細については、後述する。

【０１６３】鍵情報ヘッダ生成部１０６は、一例として、図２９に示すヘッダ情報Ｄ７００を生成する。ヘッダ情報Ｄ７００は、ＮＲＰ｛１１｝、｛００｝、｛１０｝、｛０１｝及び｛０１｝から構成され、各ＮＲＰをこの順序で含んでいる。また、この図に示すように、ヘッダ情報Ｄ７００内に「０」、「１」、「２」、「３」及び「４」により定まる位置において、それぞれ、ＮＲＰ｛１１｝、｛００｝、｛１０｝、｛０１｝及び｛０１｝が配置されている。

【０１６４】（２）鍵情報生成部１０７

鍵情報生成部１０７は、一例として、図３０に示す鍵情報Ｄ８００を生成する。鍵情報Ｄ８００は、３個の暗号化メディア鍵を含んでいる。３個の暗号化メディア鍵は、それぞれデバイス鍵ＫｅｙＧ、ＫｅｙＬ、ＩＫ１１を用いてメディア鍵を暗号化したものである。

【０１６５】これらの複数個の暗号化メディア鍵のそれぞれは、鍵情報Ｄ８００内において格納されている位置が定められている。この図に示すように、鍵情報Ｄ８００内に「０」、「１」及び「２」により定まる位置において、それぞれ、暗号化メディア鍵Ｅ１（ＫｅｙＧ、メディア鍵）、Ｅ１（ＫｅｙＬ、メディア鍵）及びＥ１（ＩＫ１１、メディア鍵）が配置されている。

【０１６６】３．１．２　記録装置３００ａ

著作物保護システム１０ｃの記録装置３００ａは、第１の実施の形態において述べた記録装置３００ａと同様の構成を有している。ここでは、その相違点を中心として説明する。

（１）特定部３０３

特定部３０３は、ＩＤ情報及びヘッダ情報を用いて、ヘッダ情報を上位からシーケンシャルに調べていくことにより、鍵情報の中から１個の暗号化メディア鍵が存在する位置Ｘを特定する。なお、暗号化メディア鍵が存在する位置Ｘを特定する場合の詳細の動作については、後述する。

【０１６７】３．２　著作物保護システム１０ｃの動作

著作物保護システム１０ｃの動作について、著作物保護システム１０の動作との相違点を中心として説明する。

３．２．１　ヘッダ情報の生成の動作

ここでは、鍵情報ヘッダ生成部１０６によるヘッダ情報の生成の動作について、図３１～図３４に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図１１に示すフローチャートにおけるステップＳ１５３の詳細である。

【０１６８】鍵情報ヘッダ生成部１０６は、レイヤ０からレイヤ３までの各レイヤについて、ステップＳ３２２～Ｓ３２７を繰り返す。さらに、鍵情報ヘッダ生成部１０６は、各レイヤに含まれる対象ノード毎に、ステップＳ３２３～Ｓ３２６ａを繰り返す。鍵情報ヘッダ生成部１０６は、当該対象ノードの直下に接続される２個の下位ノードを選択し（ステップＳ３２３）、選択した２個の下位ノードのそれぞれに無効化フラグが付されているか否かを調べて、ＮＲＰを生成し（ステップＳ３２４）、生成されたＮＲＰを木構造テーブル内の当該対象ノードに対応するノード情報内に付加する（ステップＳ２３６ａ）。

【０１６９】以上のようにして、ステップＳ３２１～Ｓ３２８の繰返しが終了すると、第１の実施の形態において説明した方法と同様に、各ノードにＮＲＰが付加される。次に、鍵情報ヘッダ生成部１０６は、レイヤ３からレイヤ０までの各レイヤについて、ステップＳ３３０～Ｓ３３５を繰り返す。さらに、鍵情報ヘッダ生成部１０６は、各レイヤに含まれる対象ノード毎に、ステップＳ３３１～Ｓ３３４ａを繰り返す。

【０１７０】鍵情報ヘッダ生成部１０６は、当該対象ノードの直下に接続される２個の下位ノードを選択し（ステップＳ３３１）、選択した２個のノードの両方にそれぞれＮＲＰ｛１１｝が付加されているか否かを調べる。ただし、選択した２個のノードがリーフである場合には、選択した２個のノードの両方に無効化フラグが付されているか否かを調べる（ステップＳ３３２）。

【０１７１】選択した２個の下位ノードの両方にそれぞれＮＲＰ｛１１｝が付されている場合にのみ、ただし選択した２個のノードがリーフである場合には、選択した２個の下位ノードの両方に無効化フラグが付されている場合にのみ（ステップＳ３３３）、鍵情報ヘッダ生成部１０６は、当該対象ノードに付加されたＮＲＰを｛００｝に書き換える（ステップＳ３３４ａ）。

【０１７２】以上のようにして、ステップＳ３２９～Ｓ３３６の繰返しが終了すると、それぞれＮＲＰ｛１１｝が付加されている２個の下位ノードに接続する上位のノードには、｛００｝が付加されることになる。次に、鍵情報ヘッダ生成部１０６は、レイヤ２からレイヤ０までの各レイヤについて、ステップＳ３３８～Ｓ３４３を繰り返す。さらに、鍵情報ヘッダ生成部１０６は、各レイヤに含まれる対象ノード毎に、ステップＳ３３９～Ｓ３４２ａを繰り返す。

【０１７３】鍵情報ヘッダ生成部１０６は、当該対象ノードの直下に接続される２個の下位ノードを選択し（ス

テップＳ３３９）、選択した２個の下位ノードの両方にＮＲＰ｛００｝が付加されているか否かを調べる（ステップＳ３４０ａ）。選択した２個の下位ノードの両方にＮＲＰ｛００｝が付加されている場合にのみ（ステップＳ３４１ａ）、鍵情報ヘッダ生成部１０６は、選択した２個の下位ノードにそれぞれ付加されたＮＲＰを木構造テーブルから削除する（ステップＳ３４２ａ）。

【０１７４】次に、鍵情報ヘッダ生成部１０６は、木構造テーブルに記憶されているＮＲＰをルートから順に読み出して、出力する（ステップＳ３４５）。以上のようにして、ＮＲＰが｛００｝である場合に、そのノードの子孫のノードに割り当てられたユーザ装置は全て無効化装置であることを示すＮＲＰが生成される。

【０１７５】３．２．２　鍵情報の特定の動作

ここでは、記録装置３００ａが有する特定部３０３により、記録媒体２００ｂに記憶されている鍵情報から、１個の暗号化メディア鍵を特定する動作について、図３５に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図１１に示すフローチャートにおけるステップＳ１７２の詳細である。

【０１７６】また、特定部３０３による１個の暗号化メディア鍵を特定する動作は、第１の実施の形態において説明した動作と同様であり、ここでは、その相違点を中心として説明する。値Ｂ＝０の場合（ステップＳ３０３）、特定部３０３は、これまでにチェックしたＮＲＰのうち、オール「１」でないＮＲＰの数とオール「０」でないＮＲＰの数とをカウントする。ただし、レイヤ０に関してのみ、オール「０」のＮＲＰもカウントする。カウントした値を、変数Ｘに代入する。こうして得られた変数Ｘが、暗号化メディア鍵の位置を示している。また、この時点の変数Ｉは、デバイス鍵を識別するためのデバイス鍵識別情報である（ステップＳ３０７ｂ）。次に、特定部３０３は、処理を終了する。

【０１７７】３．２．３　鍵情報の特定の動作の具体例

一具体例として、図２９及び図３０に示す鍵情報を用いて、図２８に示す無効化されていないユーザ装置１０が暗号化メディア鍵を特定するまでの動作について以下に説明する。ユーザ装置１０には、ＩＤ情報「１００１」が割り当てられ、デバイス鍵「ＫｅｙＡ」、「ＫｅｙＣ」、「ＫｅｙＦ」、「ＫｅｙＬ」及び「ＩＫ１０」が割り当てられているものとする。

【０１７８】（ステップ１）特定部３０３は、ユーザ装置１０に割り当てられたＩＤ情報「１００１」の最上位ビットの値が「１」であるため、最初のＮＲＰ｛１１｝の右ビットをチェックする（ステップＳ３０３）。

（ステップ２）最初のＮＲＰ｛１１｝の右ビットの値が「１」であるため、特定部３０３は、解析を続ける（ステップＳ３０３で、Ｂ＝１）。

【０１７９】（ステップ３）特定部３０３は、レイヤ０に存在する１個のＮＲＰ｛１１｝の「１」の数をカウントする。そのカウントした値が「２」であるため、次のレイヤ１には２個のＮＲＰが存在することが分かる（ステップＳ３０４）。

（ステップ４）特定部３０３は、対応するビット位置までのＮＲＰの「１」の数をカウントする。ただし、対応するビット位置の値はカウントしない。そのカウントした値が「１」であるため、次のレイヤ１の対応するＮＲＰの位置は、レイヤ１内において、１番目である（ステップＳ３０５）。

【０１８０】（ステップ５）次に、特定部３０３は、ＩＤ情報「１００１」の上位から２ビット目の値が「０」であるため、レイヤ１の１番目のＮＲＰ｛１０｝の左ビットをチェックする（ステップＳ３０３）。

（ステップ６）レイヤ１の１番目のＮＲＰ｛１０｝の左ビットの値が「１」であるため、特定部３０３は、解析を続ける（ステップＳ３０５で、Ｂ＝１）。

【０１８１】（ステップ７）特定部３０３は、レイヤ１に存在する２個のＮＲＰの「１」の数をカウントする。ここで、ＮＲＰ｛００｝は、カウントしない。そのカウントした値が「１」であるため、次のレイヤ２には１個のＮＲＰが存在することが分かる（ステップＳ３０４）。

（ステップ８）特定部３０３は、対応するビット位置までのＮＲＰの「１」の数をカウントする。ただし、対応するビット位置の値はカウントしない。そのカウントした値が「０」であるため、次のレイヤ２の対応するＮＲＰの位置は、レイヤ２内において、０番目である（ステップＳ３０５）。

【０１８２】（ステップ９）次に、特定部３０３は、ＩＤ情報「１００１」の上位から３ビット目の値が「０」であるため、レイヤ２の０番目のＮＲＰ｛０１｝の下位２ビットのうちの左ビットをチェックする（ステップＳ３０３）。

（ステップ１０）ここで、レイヤ２の０番目のＮＲＰ｛０１｝の下位２ビットのうちの左ビットの値が「０」であるため、特定部３０３は、解析を終了する（ステップＳ３０３で、Ｂ＝０）。

【０１８３】（ステップ１１）特定部３０３は、これまでに解析したＮＲＰのうち、オール「１」でないＮＲＰの数をカウントする。なお、最後にチェックしたＮＲＰはカウントしない。カウントした値が「１」であるため、暗号化メディア鍵の位置は、鍵情報内において、１番目である。

（ステップ１２）図３０より、鍵情報の１番目の位置に格納されている暗号化メディア鍵は、Ｅ１（ＫｅｙＬ，メディア鍵）である。

【０１８４】ユーザ装置１０は、ＫｅｙＬを保持している。よって、ユーザ装置１０は、ＫｅｙＬを用いて暗号化メディア鍵を復号してメディア鍵を獲得することができる。

４．第４の実施の形態

上記の第１の実施の形態においては、複数のＮＲＰを上位レイヤから下位レイヤの順に並べ、レイヤが同じＮＲＰについては、左から右への順に並べるようにしている。

【０１８５】次に述べる第４の実施の形態では、別の並べ方により複数のＮＲＰを出力する著作物保護システム１０ｄ（図示していない）について説明する。

４．１　著作物保護システム１０ｄの構成

著作物保護システム１０ｄは、著作物保護システム１０と同様の構成を有している。ここでは、著作物保護システム１０との相違点を中心として説明する。

【０１８６】４．１．１　鍵管理装置１００

著作物保護システム１０ｄの鍵管理装置１００は、第１の実施の形態において述べた鍵管理装置１００と同様の構成を有している。ここでは、その相違点を中心として説明する。

（１）木構造格納部１０２

木構造格納部１０２は、具体的にはハードディスクユニットから構成されており、図３７に一例として示すように木構造テーブルＤ１０００を有している。

【０１８７】木構造テーブルＤ１０００は、図３６に一例として示す木構造Ｔ６００に対応しており、木構造Ｔ６００を表現するためのデータ構造を示す。後述するように、木構造構築部１０１により木構造Ｔ６００を表現するためのデータ構造が、木構造テーブルＤ１０００として生成され、木構造格納部１０２に書き込まれる。

（木構造Ｔ６００）木構造Ｔ６００は、図３６に示すように、木構造Ｔ１００と同様に、レイヤ０からレイヤ４までの５階層からなる２分木である。

【０１８８】木構造Ｔ６００の各レイヤに含まれるノードの数は、木構造Ｔ１００と同じである。また、上位側のノードと下位側のノードを接続する経路に割り当てられる番号も、木構造Ｔ１００と同じである。木構造Ｔ６００において、×が付されているノードは、無効化されている。木構造Ｔ６００のルートであるノードのノード名は、空白である。他のノードのノード名は、木構造Ｔ１００と同様に設定される。

【０１８９】各ノード名は、４桁の文字で表現される。ルートであるノードのノード名は、４桁の空白文字からなる。ノード名「０」は、具体的には、文字「０」＋１桁の空白文字＋１桁の空白文字＋１桁の空白文字である。ノード名「００」は、文字「０」＋文字「０」＋１桁の空白文字＋１桁の空白文字である。ノード名「１０１」は、文字「１」＋文字「０」＋文字「１」＋１桁の空白文字である。ノード名「１１１１」は、文字「１」＋文字「１」＋文字「１」＋文字「１」である。その他のノード名についても同様である。

【０１９０】木構造Ｔ６００において、各ノードの付近に付された｛１０｝などは、ＮＲＰを示している。また、各ノードの付近に付された○印で囲まれた番号は、ＮＲＰが出力される順序を示している。

（木構造テーブルＤ１０００）木構造テーブルＤ１０００は、木構造Ｔ６００に含まれるノードと同じ数のノード情報を含んで構成されており、各ノード情報は、木構造Ｔ６００を構成する各ノードにそれぞれ対応している。

【０１９１】各ノード情報は、ノード名、デバイス鍵及び無効化フラグを含んでいる。ノード名、デバイス鍵及び無効化フラグについては、木構造テーブルＤ１００と同じであるので説明を省略する。木構造テーブルＤ１０００内には、次に示す順序規則２に従った順序により各ノード情報が記憶される。ここに示す順序規則２は、記録装置３００ａ、３００ｂ、３００ｃ、・・・、再生装置４００ａ、４００ｂ、４００ｃ、・・・により、木構造テーブルＤ１０００から各ノード情報がシーケンシャルに読み出される場合においても適用される。

【０１９２】（ａ）木構造テーブルＤ１０００内の先頭には、ルートであるノードに対応するノード情報が記憶される。

（ｂ）１個のノード（特定ノードと呼ぶ。）に対応するノード情報が木構造テーブルＤ１０００内に記憶された後において、前記特定ノードの下位側に接続する２個の下位ノードが存在する場合には、次に示すようにして、ノード情報が並べられる。前記特定ノードに対応するノード情報に続いて、前記２個の下位ノードのうち、左側のノード及び前記左側のノードのさらに下位側に接続する全てのノードに対応する各ノード情報が記憶される。続いて、前記２個の下位ノードのうち、右側のノード及び前記右側のノードのさらに下位側に接続する全てのノードに対応する各ノード情報が記憶される。

【０１９３】（ｃ）（ｂ）内において、（ｂ）が再度、適用される。具体的には、図３７に示す木構造テーブルＤ１００内には、次に示す順序により各ノード情報が記憶される。空白（ルートを示す）、「０」、「００」、「０００」、「００００」、「０００１」、「００１」、「００１０」、「００１１」、「０１」、「０１０」、・・・、「１１」、「１１０」、「１１００」、「１１０１」、「１１１」、「１１１０」、「１１１１」

（２）木構造構築部１０１

木構造構築部１０１は、デバイス鍵を管理するためのｎ分木データ構造を構築し、木構造格納部１０２に構築した木構造を格納する。ここで、ｎは２以上の整数であり、一例として、ｎ＝２である。

【０１９４】木構造構築部１０１による木構造の構築及び木構造格納部１０２への格納の詳細の動作については、後述する。木構造構築部１０１は、次に、木構造のノード毎に乱数を用いてデバイス鍵を生成し、生成したデバイス鍵を各ノードに対応付けて木構造テーブル内に

書き込む。

【０１９５】（３）鍵情報ヘッダ生成部１０６

鍵情報ヘッダ生成部１０６は、複数のＮＲＰを生成し、生成した複数のＮＲＰをヘッダ情報として、鍵情報記録装置２００へ出力する。ＮＲＰの生成の詳細の動作については、後述する。鍵情報ヘッダ生成部１０６により生成されるヘッダ情報の一例を図３８に示す。この図に示すヘッダ情報Ｄ９００は、ＮＲＰ｛１１｝、｛１１｝、｛１１｝、｛１０｝、｛０１｝、｛１１｝、｛１０｝、｛１０｝、｛１０｝、｛０１｝、｛１１｝から構成され、各ＮＲＰをこの順序で含んでいる。

【０１９６】なお、これらの複数個のＮＲＰのそれぞれは、ヘッダ情報Ｄ９００内において格納されている位置が定められている。この図に示すように、ヘッダ情報Ｄ９００内に「０」、「１」、「２」、「３」、「４」、「５」、「６」、「７」、「８」、「９」、「１０」、により定まる位置において、それぞれ、ＮＲＰ｛１１｝、｛１１｝、｛１１｝、｛１０｝、｛０１｝、｛１１｝、｛１０｝、｛１０｝、｛１０｝、｛０１｝、｛１１｝が配置されている。

【０１９７】（４）鍵情報生成部１０７

鍵情報生成部１０７は、上記の木構造テーブルにノード情報が格納される順序と同じ順序で、無効化されていないノードに対応するデバイス鍵を用いて、メディア鍵を暗号化して暗号化メディア鍵を生成し、生成した暗号化メディア鍵を鍵情報として出力する。

【０１９８】鍵情報生成部１０７は、一例として次に示す鍵情報を生成して出力する。鍵情報は、デバイス鍵「ＩＫ２」、「ＩＫ３」、「ＩＫ６」、「ＩＫ８」、「ＫｅｙＬ」及び「ＫｅｙＧ」をそれぞれ用いて、メディア鍵を暗号化することにより、生成された暗号化メディア鍵Ｅ１（ＩＫ２、メディア鍵）、Ｅ１（ＩＫ３、メディア鍵）、Ｅ１（ＩＫ６、メディア鍵）、Ｅ１（ＩＫ８、メディア鍵）、Ｅ１（ＫｅｙＬ、メディア鍵）及びＥ１（ＫｅｙＧ、メディア鍵）から構成されている。この鍵情報内に、「０」、「１」、「２」、「３」、「４」、「５」及び「６」により定まる位置において、それぞれ、暗号化メディア鍵Ｅ１（ＩＫ２、メディア鍵）、Ｅ１（ＩＫ３、メディア鍵）、Ｅ１（ＩＫ６、メディア鍵）、Ｅ１（ＩＫ８、メディア鍵）、Ｅ１（ＫｅｙＬ、メディア鍵）及びＥ１（ＫｅｙＧ、メディア鍵）が配置されている。

【０１９９】４．１．２　記録装置３００ａ

著作物保護システム１０ｄの記録装置３００ａは、第１の実施の形態において述べた記録装置３００ａと同様の構成を有している。ここでは、その相違点を中心として説明する。

（１）特定部３０３

特定部３０３は、ＩＤ情報及びヘッダ情報を用いて、ヘッダ情報を上位からシーケンシャルに調べていくことにより、鍵情報の中から１個の暗号化メディア鍵が存在する位置Ｘを特定する。なお、暗号化メディア鍵が存在する位置Ｘを特定する場合の詳細の動作については、後述する。

【０２００】４．２　著作物保護システム１０ｄの動作

著作物保護システム１０ｄの動作については、著作物保護システム１０の動作との相違点を中心として説明する。

４．２．１　木構造を構築して格納する動作

ここでは、木構造構築部１０１による木構造テーブルの生成と木構造格納部１０２への木構造テーブルの書き込みの動作について、図３９に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図１０に示すフローチャートにおけるステップＳ１０１の詳細である。

【０２０１】木構造構築部１０１は、空白のノード名を含むノード情報を生成して木構造テーブルに書き込む（ステップＳ４０１）。次に、木構造構築部１０１は、レイヤｉ（ｉ＝１、２、３、４）について、次に示すステップＳ４０３～ステップＳ４０４を繰り返す。木構造構築部１０１は、２ｉ個の文字列をノード名として生成する。具体的には、ｉ＝１のときは、２１＝２個の文字列「０」及び「１」を生成する。また、ｉ＝２のときは、２２＝４個の文字列「００」、「０１」、「１０」及び「１１」を生成する。また、ｉ＝３のときは、２３＝８個の文字列「０００」、「００１」、「０１０」、・・・・、「１１１」を生成する。また、ｉ＝４のときは、２４＝１６個の文字列「００００」、「０００１」、「００１０」、「００１１」、・・・・、「１１１１」を生成する（ステップＳ４０３）。次に、木構造構築部１０１は、生成した各ノード名をそれぞれ含むノード情報を木構造テーブルに書き込む（ステップＳ４０４）。

【０２０２】次に、木構造構築部１０１は、木構造テーブルに含まれている各ノード情報を、ノード名の昇順に並び換え、並び替えられた各ノード情報を再度、木構造テーブルに上書きする（ステップＳ４０６）。このようにして、図３７に一例として示す木構造テーブルＤ１００００が生成される。生成された木構造テーブルＤ１０００ｈは、上述した順序規則２により各ノード情報を含んでいる。なお、この段階では、木構造テーブルＤ１０００内に各デバイス鍵はまだ記録されていない。

【０２０３】４．２．２　ヘッダ情報の生成の動作

ここでは、鍵情報ヘッダ生成部１０６によるヘッダ情報の生成の動作について、図４０～図４１に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図１１に示すフローチャートにおけるステップＳ１５３の詳細である。

【０２０４】鍵情報ヘッダ生成部１０６は、順序規則２に従って木構造テーブルから順に１個ずつノード情報の読出しを試みる（ステップＳ４２１）。ノード情報の終

了を検出すると（ステップＳ４２２）、鍵情報ヘッダ生成部１０６は、ステップＳ４２７へ制御を移す。ノード情報の終了を検出せず、ノード情報が読み出せた場合には（ステップＳ４２２）、鍵情報ヘッダ生成部１０６は、読み出したノード情報に対応する対象ノードの下位側に接続されている２個の下位ノードに対応する２個のノード情報を読み出す（ステップＳ４２３）。

【０２０５】下位ノードが存在する場合に（ステップＳ４２４）、鍵情報ヘッダ生成部１０６は、読み出した２個の下位ノードに対応する２個のノード情報の両方に、無効化フラグが付されているか否かを調べて、ＮＲＰを生成し（ステップＳ４２５）、次に、生成したＮＲＰを読み出した対象ノードに対応するノード情報に付加する（ステップＳ４２６）。次に、ステップＳ４２１へ戻って処理を繰り返す。

【０２０６】下位ノードが存在しない場合（ステップＳ４２４）、ステップＳ４２１へ戻って処理を繰り返す。次に、鍵情報ヘッダ生成部１０６は、順序規則２に従って木構造テーブルから順に１個ずつノード情報の読出しを試みる（ステップＳ４２７）。ノード情報の終了を検出すると（ステップＳ４２２）、鍵情報ヘッダ生成部１０６は、処理を終了する。

【０２０７】ノード情報の終了を検出せず、ノード情報が読み出せた場合には（ステップＳ４２８）、鍵情報ヘッダ生成部１０６は、読み出したノード情報にＮＲＰが付加されているか否かを調べ、付加されている場合（ステップＳ４２９）、付加されているＮＲＰを出力し（ステップＳ４３０）、次に、ステップＳ４２７へ戻って処理を繰り返す。

【０２０８】ＮＲＰが付加されていない場合（ステップＳ４２９）、鍵情報ヘッダ生成部１０６は、ステップＳ４２７へ戻って処理を繰り返す。

４．２．３　鍵情報の特定の動作

ここでは、記録装置３００ａが有する特定部３０３により、記録媒体５００ｂに記憶されている鍵情報から、１個の暗号化メディア鍵を特定する動作について、図４２に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図１１に示すフローチャートにおけるステップＳ１７２の詳細である。

【０２０９】また、再生装置４００ａが有する特定部４０２による動作は、特定部３０３による動作と同じであるので、説明を省略する。特定部３０３は、チェックするＩＤ情報のビット位置を示す変数ｉ、現在チェックしているＮＲＰが含まれるレイヤを示す変数Ｌ、分岐点のノードのレイヤを記憶する変数Ｘ、ＮＲＰをチェックするか否かを判断するフラグＦ（初期値、Ｆ＝０）を有しており、木構造のレイヤ数を示す値Ｄを有している。また、チェックするＮＲＰの位置を示すポインタＡを有している。

【０２１０】特定部３０３は、変数ｉ＝０、変数Ｌ＝０、フラグＦ＝０、変数Ｘ＝０、ポインタＡ＝０とする（ステップＳ１３００）。次に、特定部３０３は、変数Ｌがレイヤ数Ｄ－１よりも小さいか否かを判定する。大きいか又は等しい場合（ステップＳ１３０１）、特定部３０３は、変数Ｌに対して、変数Ｘの最後のレイヤ番号を入力する。変数Ｘは、後入れ先出しの変数であり、出力した値は削除されるものとする。即ち、変数Ｘにレイヤ０、レイヤ２、レイヤ３の順で入力されたとすると、最初に出力されるのはレイヤ３で、そのレイヤ３は削除され、次はレイヤ２が出力される（ステップＳ１３１３）。次に、ステップＳ１３０１へ戻って処理を繰り返す。

【０２１１】変数Ｌがレイヤ数Ｄ－１よりも小さい場合（ステップＳ１３０１）、特定部３０３は、変数ｉ＝変数Ｌであるか否かを判定する。変数ｉ＝変数Ｌでない場合（ステップＳ１３０２）、特定部３０３は、ステップＳ１３１０へ制御を移す。変数ｉ＝変数Ｌである場合（ステップＳ１３０２）、特定部３０３は、さらに、フラグＦ＝０であるか否かを判定する。フラグＦ＝０でない場合（ステップＳ１３０３）、特定部３０３は、フラグＦ＝０とし（ステップＳ１３０９）、特定部３０３は、ステップＳ１３１０へ制御を移す。

【０２１２】フラグＦ＝０である場合（ステップＳ１３０３）、特定部３０３は、ＩＤ情報の上位ｉビット目の値に従って、Ａ番目のＮＲＰの対応するビット位置の値Ｂをチェックし、変数ｉ＝ｉ＋１とする（ステップＳ１３０４）。次に、特定部３０３は、値Ｂ＝１であるか否かを調べ、値Ｂ＝１でない場合（ステップＳ１３０５）、このＩＤ情報が割り当てられた装置は無効化されていないものとして、特定部３０３は、処理を終了する。

【０２１３】値Ｂ＝１である場合（ステップＳ１３０５）、変数≠Ｄ－１であるか否かを調べ、変数≠Ｄ－１でない場合（ステップＳ１３０６）、このＩＤ情報が割り当てられた装置は無効化されているものとして、特定部３０３は、処理を終了する。次に、変数≠Ｄ－１である場合（ステップＳ１３０６）、特定部３０３は、ＮＲＰが｛１１｝であり、かつＩＤ情報のｉ－１番目の値が「１」であるか否かを判定する。Ｎｏの場合（ステップＳ１３０７）、特定部３０３は、ステップＳ１３１０へ制御を移す。

【０２１４】Ｙｅｓの場合（ステップＳ１３０７）、特定部３０３は、フラグＦ＝１とし（ステップＳ１３０８）、次に、Ｌ＝Ｌ＋１とし（ステップＳ１３１０）、ＮＲＰが｛１１｝であれば、そのレイヤ番号を変数Ｘに記憶し（ステップＳ１３１１）、Ａ＝Ａ＋１とし（ステップＳ１３１２）、次に、ステップＳ１３１０へ戻って処理を繰り返す。

【０２１５】５．第５の実施の形態

上記の第４の実施の形態においては、複数のＮＲＰを順

序規則２により並べるようにしている。次に述べる第５の実施の形態では、第４の実施の形態において述べた著作物保護システム１０ｄと同様に、順序規則２により並べて複数のＮＲＰを出力し、かつ、第２の実施の形態において述べた著作物保護システム１０ｂと同様に、無効化された装置が木構造の中で特定のリーフに集中する場合に、ヘッダ情報のデータ量を少なく抑えることができる著作物保護システム１０ｅ（図示していない）について説明する。

【０２１６】５．１　著作物保護システム１０ｅの構成

著作物保護システム１０ｅは、著作物保護システム１０ｄと同様の構成を有している。ここでは、著作物保護システム１０ｄとの相違点を中心として説明する。

５．１．１　鍵管理装置１００

著作物保護システム１０ｅの鍵管理装置１００は、第４の実施の形態において述べた鍵管理装置１００ｄと同様の構成を有している。ここでは、その相違点を中心として説明する。

【０２１７】（１）木構造格納部１０２

木構造格納部１０２は、木構造テーブルを有している。木構造格納部１０２が有する木構造テーブルは、第４の実施の形態において説明した木構造格納部１０２が有している木構造テーブルＤ１０００と同様の構造を備えており、木構造テーブルに含まれる各ノード情報は、さらに、ＮＲＰを含む。

【０２１８】（２）鍵情報ヘッダ生成部１０６

鍵情報ヘッダ生成部１０６は、複数のＮＲＰを生成し、生成した複数のＮＲＰをヘッダ情報として、鍵情報記録装置２００へ出力する。各ＮＲＰは、第２の実施の形態において説明したように、３ビットから構成される。ＮＲＰの生成の詳細の動作については、後述する。

【０２１９】５．１．２　記録装置３００ａ

著作物保護システム１０ｅの記録装置３００ａは、第４の実施の形態において述べた記録装置３００ａと同様の構成を有している。ここでは、その相違点を中心として説明する。

（ｉ）特定部３０３

特定部３０３は、ＩＤ情報及びヘッダ情報を用いて、ヘッダ情報を上位からシーケンシャルに調べていくことにより、鍵情報の中から１個の暗号化メディア鍵が存在する位置Ｘを特定する。なお、暗号化メディア鍵が存在する位置Ｘを特定する場合の詳細の動作については、後述する。

【０２２０】５．２　著作物保護システム１０ｅの動作

著作物保護システム１０ｅの動作について、著作物保護システム１０ｄの動作との相違点を中心として説明する。

５．２．１　ヘッダ情報の生成の動作

ここでは、鍵情報ヘッダ生成部１０６によるヘッダ情報の生成の動作について、図４３～図４６に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図１１に示すフローチャートにおけるステップＳ１５３の詳細である。

【０２２１】鍵情報ヘッダ生成部１０６は、順序規則２に従って木構造テーブルから順に１個ずつノード情報の読出しを試みる（ステップＳ４５１）。ノード情報の終了を検出すると（ステップＳ４５２）、鍵情報ヘッダ生成部１０６は、ステップＳ４５８へ制御を移す。ノード情報の終了を検出せず、ノード情報が読み出せた場合には（ステップＳ４５２）、鍵情報ヘッダ生成部１０６は、読み出したノード情報に対応する対象ノードの下位側に接続されている２個の下位ノードに対応する２個のノード情報を読み出す（ステップＳ４５３）。

【０２２２】下位ノードが存在する場合に（ステップＳ４５４）、鍵情報ヘッダ生成部１０６は、読み出した２個の下位ノードに対応する２個のノード情報の両方に、無効化フラグが付されているか否かを調べて、ＮＲＰを生成し（ステップＳ４５５）、値「０」を有する拡張ビットを生成したＮＲＰの先頭に付加し（ステップＳ４５６）、次に、拡張ビットの付加されたＮＲＰを読み出した対象ノードに対応するノード情報に付加する（ステップＳ４５７）。次に、ステップＳ４５１へ戻って処理を繰り返す。

【０２２３】下位ノードが存在しない場合（ステップＳ４５４）、ステップＳ４５１へ戻って処理を繰り返す。次に、鍵情報ヘッダ生成部１０６は、順序規則２に従って木構造テーブルから順に１個ずつノード情報の読出しを試みる（ステップＳ４５８）。ノード情報の終了を検出すると（ステップＳ４５９）、鍵情報ヘッダ生成部１０６は、ステップＳ４６５へ制御を移す。

【０２２４】ノード情報の終了を検出せず、ノード情報が読み出せた場合には（ステップＳ４５９）、鍵情報ヘッダ生成部１０６は、読み出したノード情報に対応する対象ノードの下位側に接続されている全ての下位ノードに対応する全てのノード情報を読み出す（ステップＳ４６０）。下位ノードが存在する場合に（ステップＳ４６１）、鍵情報ヘッダ生成部１０６は、読み出した全ての下位ノードに対応する全てのノード情報に、無効化フラグが付されているか否かを調べ（ステップＳ４６２）、全てのノード情報に付加されている場合にのみ（ステップＳ４６３）、対象ノードに対応するノード情報に付加されたＮＲＰの先頭ビットを「１」に書き換える（ステップＳ４６４）。

【０２２５】次に、ステップＳ４５８へ戻って処理を繰り返す。下位ノードが存在しない場合（ステップＳ４６１）、ステップＳ４５８へ戻って処理を繰り返す。次に、鍵情報ヘッダ生成部１０６は、順序規則２に従って木構造テーブルから順に１個ずつノード情報の読出しを試みる（ステップＳ４６５）。

【０２２６】ノード情報の終了を検出すると（ステップ

Ｓ４６６）、鍵情報ヘッダ生成部１０６は、ステップＳ４７２へ制御を移す。ノード情報の終了を検出せず、ノード情報が読み出せた場合には（ステップＳ４６６）、鍵情報ヘッダ生成部１０６は、読み出したノード情報に対応する対象ノードの下位側に接続されている全ての下位ノードに対応する全てのノード情報を読み出す（ステップＳ４６７）。

【０２２７】下位ノードが存在する場合に（ステップＳ４６８）、鍵情報ヘッダ生成部１０６は、読み出した全ての下位ノードに対応する全てのノード情報に、それぞれＮＲＰ｛１１１｝が付加されているか否かを調べ（ステップＳ４６９）、全てのノード情報に付加されている場合にのみ（ステップＳ４７０）、前記全てのノード情報に、それぞれ削除フラグを付加する（ステップＳ４７１）。

【０２２８】次に、ステップＳ４６５へ戻って処理を繰り返す。下位ノードが存在しない場合（ステップＳ４６８）、ステップＳ４６５へ戻って処理を繰り返す。次に、鍵情報ヘッダ生成部１０６は、順序規則２に従って木構造テーブルから順に１個ずつノード情報の読出しを試みる（ステップＳ４７２）。

【０２２９】ノード情報の終了を検出すると（ステップＳ４７３）、鍵情報ヘッダ生成部１０６は、処理を終了する。ノード情報の終了を検出せず、ノード情報が読み出せた場合には（ステップＳ４７３）、鍵情報ヘッダ生成部１０６は、読み出したノード情報にＮＲＰが付加されているか否かを調べ、付加されている場合（ステップＳ４７４）、さらに、削除フラグが付加されているか否かを調べ、削除フラグが付加されていない場合には（ステップＳ４７５）、付加されているＮＲＰを出力し（ステップＳ４７６）、次に、ステップＳ４７２へ戻って処理を繰り返す。

【０２３０】ＮＲＰが付加されていない場合（ステップＳ４７４）、又は、削除フラグが付加されている場合（ステップＳ４７５）、鍵情報ヘッダ生成部１０６は、ステップＳ４７２へ戻って処理を繰り返す。５．２．２

鍵情報の特定の動作ここでは、記録装置３００ａが有する特定部３０３により、記録媒体５００ｂに記憶されている鍵情報から、１個の暗号化メディア鍵を特定する動作について、図４７に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図１１に示すフローチャートにおけるステップＳ１７２の詳細である。

【０２３１】また、再生装置４００ａが有する特定部４０２による動作は、特定部３０３による動作と同じであるので、説明を省略する。また、ここでは、図４２に示すフローチャートとの相違点を中心として説明する。特定部３０３は、第４の実施の形態の場合と同様に、チェックするＩＤ情報のビット位置を示す変数ｉ、現在チェックしているＮＲＰが含まれるレイヤを示す変数Ｌ、分岐点のノードのレイヤを記憶する変数Ｘ、ＮＲＰをチェックするか否かを判断するフラグＦ（初期値、Ｆ＝０）を有しており、木構造のレイヤ数を示す値Ｄを有している。また、チェックするＮＲＰの位置を示すポインタＡを有している。

【０２３２】値Ｂ＝１である場合（ステップＳ１３０５）、ＮＲＰの最上位ビットが「１」であるときにのみ（ステップＳ１３１６）、特定部３０３は、変数ｉ＝Ｄ－１とし、変数Ｌ＝Ｄ－１とする（ステップＳ１３１７）。また、特定部３０３は、ＮＲＰが｛１１｝であり、かつＮＲＰの最上位ビットが「１」でないとき、そのレイヤ番号を変数Ｘに記憶する（ステップＳ１３１１）。

【０２３３】６．その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

（１）本発明の実施の形態として、従来方式による無効化方法を例として説明したが、本発明は上記の実施の形態に限定されるものではない。鍵管理装置がある木構造を保持し、この木構造のリーフに記録装置又は再生装置を割り当て、ノードに付随するあるデバイス鍵を各記録装置又は各再生装置に割り当てるものであり、鍵管理装置がこの木構造を用いて前記デバイス鍵の無効化と、前記鍵情報の作成を行うものであれば、前記ノードに付随するデバイス鍵の割り当て方や、各装置へのデバイス鍵の割り当て方はどのようなものであってもよい。

【０２３４】（２）また、本発明の実施の形態として、２分木の木構造を例として説明したが、本発明は２分木に限定されるものではない。一般にｎ分木でも実現可能である。このときＩＤ情報は、あるノードから下に派生するｎ本の経路に対して、０～ｎ－１を割り当て、上述した実施の形態と同様に、リーフからルートに至るまでの経路上に割り当てられた値を上位から順に連結することにより、設定される。

【０２３５】（３）以上で述べた本発明の実施の形態においては、ＤＶＤ－ＲＡＭ等のレコーダブルメディアについて説明した。しかし、ＤＶＤ－Ｖｉｄｅｏ等のプレレコーディッドメディアについても、同様の方法で実現することができる。プレレコーディッドメディアにおける著作物保護システムＩＯｆについて、説明する。

【０２３６】著作物保護システムＩＯｆは、図４８に示すように、鍵管理装置１００、データ記録装置１７０１、データ再生装置１７０３ａ、１７０３ｂ、１７０３ｃ、・・・から構成されている。鍵管理装置１００は、上記の実施の形態において説明したように、ヘッダ情報が付加された鍵情報とコンテンツ鍵とをデータ記録装置１７０１へ出力し、複数のデバイス鍵と各デバイス鍵識別情報とＩＤ情報とをデータ再生装置１７０３ａ、１７０３ｂ、１７０３ｃ、・・・へ出力する。

【０２３７】データ記録装置１７０１に、プレレコーディッドメディアである記録媒体５００ａが装着される。データ記録装置１７０１は、鍵管理装置１００から鍵情報とメディア鍵とを受け取り、メディア鍵を用いてコンテンツを暗号化して暗号化コンテンツを生成し、生成した暗号化コンテンツと受け取った鍵情報とを記録媒体５００ａに書き込む。こうして、暗号化コンテンツと鍵情報とが書き込まれた記録媒体５００ｄが生産される。

【０２３８】記録媒体５００ｄは、市場を流通し、利用者は、記録媒体５００ｄを入手する。利用者は、記録媒体５００ｄをデータ再生装置１７０３ａに装着する。データ再生装置１７０３ａは、鍵管理装置１００から複数のデバイス鍵と各デバイス鍵識別情報とＩＤ情報とを予め受け取っており、記録媒体５００ｄが装着されると、記録媒体５００ｄから鍵情報と暗号化コンテンツとを読み出し、鍵情報から暗号化メディア鍵を特定し、特定した暗号化メディア鍵をデバイス鍵を用いて復号し、得られたメディア鍵を用いて、暗号化コンテンツを復号して、コンテンツを生成する。

【０２３９】このようなシステムにおいても、実施の形態で示した鍵管理装置１００と同様の動作により、記録媒体に記録するヘッダ情報を少なく抑えつつ、各データ再生装置で効率よく復号すべき暗号化メディア鍵を特定することができる。

（４）以上では本発明をデジタルコンテンツの著作権保護のために用いる場合を例示したが、本発明の応用はこれに限定されるものではなく、例えば、会員制の情報提供システムにおいて、ある特定の会員以外に情報を提供するという、いわゆるコンディショナルアクセスの目的にも利用できる。

【０２４０】（５）本発明の実施の形態においては、鍵情報あるいは暗号化コンテンツを、記録媒体を用いて配布する例を示したが、記録媒体の代わりに、インターネットに代表されるような通信媒体を用いてもよい。

（６）鍵管理装置と鍵情報記録装置が一体の装置から構成されているとしてもよい。

【０２４１】（７）上記の実施の形態では、ｎ分木を構成する全てのノードに予めデバイス鍵を割り当てておき、リーフからルートへの経路上に存在する全てのデバイス鍵を、前記リーフに対応する利用装置に割り当てるとしているが、本発明は、このようなデバイス鍵の割り当て方法には、限定されない。ｎ分木を構成する全てのノードに予めデバイス鍵を割り当てておくのではなく、一部のノードにのみ、予めデバイス鍵を割り当てておくとしてもよい。

【０２４２】また、リーフからルートへの経路上に存在する全てのデバイス鍵を、前記リーフに対応する利用装置に割り当てるのではなく、リーフからルートへの経路上に存在する全てのデバイス鍵のうちの一部のデバイス鍵を前記利用装置に割り当てるとしてもよい。

（８）一例として図４に示す木構造を想定する。デバイス鍵が漏洩していない初期状態では、メディア鍵は、デバイス鍵ＫｅｙＡを用いて暗号化され、暗号化メディア鍵が生成される。

【０２４３】このとき、ユーザ装置１～１６のいずれかの装置が、悪意のある第三者によりハックされて、デバイス鍵ＫｅｙＡが暴露され、デバイス鍵ＫｅｙＡだけを内部に有するクローン機器が製造されたとする。このとき、前記クローン機器は、デバイス鍵ＫｅｙＡだけを有するので、ユーザ装置１～１６のうちのどの装置がハックされた装置であるかを特定することはできない。一方で、前記クローン機器は、デバイス鍵ＫｅｙＡを有しているので、正しいメディア鍵を不正に得ることができる。

【０２４４】このような状況では、デバイス鍵ＫｅｙＡのみを無効化し、かつ、全ての機器がカバーされるようなデバイス鍵を用いて、言い換えると、全ての機器が共有しているデバイス鍵を用いて、メディア鍵を暗号化しなければならない。ここで、全ての機器をカバーする理由は、このような状況では、ハックされた機器がどの機器か断定できないためである。

【０２４５】そこで、デバイス鍵ＫｅｙＢ及びＫｅｙＣをそれぞれ用いて、メディア鍵を暗号化して２個の暗号化メディア鍵を生成する。次に、デバイス鍵ＫｅｙＢが暴露された場合には、デバイス鍵ＫｅｙＢを無効化し、さらに、デバイス鍵ＫｅｙＣ、ＫｅｙＤ及びＫｅｙＥをそれぞれ用いて、メディア鍵を暗号化して３個の暗号化メディア鍵を生成する。

【０２４６】このような操作が、木の高さ分だけ繰り返される、最終的には、ハックされた機器が特定される。以上説明したような状況に対応するために、デバイス鍵ＫｅｙＡのみを無効化する場合、鍵管理装置は、デバイス鍵ＫｅｙＡが対応するノードに対して、ＮＲＰ｛１００｝を付加する。図４に示す木構造の場合には、ルートに対して、ＮＲＰ｛１００｝を付加する。

【０２４７】ＮＲＰ｛１００｝の先頭のビット「１」は、このノードが無効化されていることを示し、また、先頭のビット「１」に続くビット列「００」は、このノードの下に接続されている２個のノードは、両方とも、無効化されていないことを示している。つまり、図４に示す木構造の場合に、ルートに対して、ＮＲＰ｛１００｝が付加されているならば、デバイス鍵ＫｅｙＢ及びＫｅｙＣを用いて、メディア鍵を暗号化して生成された２個の暗号化メディア鍵が存在することとなる。このように、ＮＲＰの先頭のビット「１」は、このノードの下には、暗号化メディア鍵が２個存在することを意味するフラグであるといえる。

【０２４８】一方、第２の実施の形態で説明したように、ＮＲＰが｛１１１｝であるときの先頭のビット「１」は、このノードの下には、ＮＲＰが存在しないこ

とを示している。以下において、さらに詳細に説明する。

（鍵管理装置１００）ここでは、鍵管理装置１００は、図４に示す木構造Ｔ１００を生成し、この図に示すように、各ノードにデバイス鍵を割り当て、各リーフにユーザ装置を割り当てたものとする。

【０２４９】この後、図４９に示すように、ルートＴ７０１、ノードＴ７０２及びノードＴ７０３にそれぞれ割り当てられたデバイス鍵ＫｅｙＡ、ＫｅｙＢ及びＫｅｙＥが、上記に示すように漏洩したため、鍵管理装置１００は、以下に示すようにして、デバイス鍵ＫｅｙＡ、ＫｅｙＢ及びＫｅｙＥを無効化し、ヘッダ情報及び鍵情報を生成し、生成したヘッダ情報及び鍵情報を、鍵情報記録装置２００を介して、記録媒体に書き込む。

【０２５０】（ａ）デバイス鍵ＫｅｙＡ、ＫｅｙＢ及びＫｅｙＥの無効化

鍵管理装置１００は、木構造テーブルにおいて、デバイス鍵ＫｅｙＡ、ＫｅｙＢ及びＫｅｙＥがそれぞれ含まれるノード情報に無効化フラグ「１」を付加する。

（ｂ）ヘッダ情報の生成

鍵管理装置１００は、無効化フラグが付加されたノード情報を含む前記木構造テーブルを用いて、ルートＴ７０１に付加するＮＲＰ｛０１０｝を生成し、生成したＮＲＰ｛０１０｝をヘッダ情報の一部として、鍵情報記録装置２００を介して、記録媒体に書き込む。ここで、ＮＲＰの先頭のビット「０」は、ルートＴ７０１の直下に接続される２個の下位のノードのいずれか一方が無効化され、他方は無効化されていないことを示している。また、ＮＲＰの下位の２ビット「１０」は、上記の実施の形態においても説明したように、ルートＴ７０１の直下に接続される２個の下位のノードのうち、左側のノードＴ７０２は、無効化されており、右側のノードＴ７０４は、無効化されていないことを示している。

【０２５１】次に、鍵管理装置１００は、ノードＴ７０２に付加するＮＲＰ｛００１｝を生成し、生成したＮＲＰ｛００１｝をヘッダ情報の一部として、鍵情報記録装置２００を介して、記録媒体に書き込む。ここで、ＮＲＰの先頭のビット「０」は、ノードＴ７０２の直下に接続される２個の下位のノードのいずれか一方が無効化され、他方は無効化されていないことを示している。また、ＮＲＰの下位の２ビット「０１」は、ノードＴ７０２の直下に接続される２個の下位のノードのうち、左側のノードＴ７０５は、無効化されておらず、右側のノードＴ７０３は、無効化されていることを示している。

【０２５２】次に、鍵管理装置１００は、ノードＴ７０３に付加するＮＲＰ｛１００｝を生成し、生成したＮＲＰ｛１００｝をヘッダ情報の一部として、鍵情報記録装置２００を介して、記録媒体に書き込む。ＮＲＰ｛１００｝は、上記において説明したように、ノードＴ７０３の直下に接続される２個の下位のノードＴ７０６、Ｔ７０７の両方とも無効化されておらず、これら２個のノードＴ７０６、Ｔ７０７には、それぞれ暗号化メディア鍵が存在することを示している。

【０２５３】このようにして、図５０に示すヘッダ情報Ｄｉ０００が記録媒体に書き込まれる。ヘッダ情報Ｄｉ０００は、この図に示すように、ＮＲＰ｛０１０｝、｛００１｝、｛１００｝をこの順序で含んで構成されている。

（ｃ）鍵情報の生成

次に、鍵管理装置１００は、以下に示すようにして、無効化されていないデバイス鍵のうちの一部のデバイス鍵を用いて、メディア鍵を暗号化して暗号化メディア鍵を生成し、生成した暗号化メディア鍵を含む鍵情報とＮＲＰを含むヘッダ情報とを、鍵情報記録装置２００を介して、記録媒体に書き込む。

【０２５４】最初に、鍵管理装置１００は、無効化されていないデバイス鍵のうち、最上位のレイヤに存在するノードに割り当てられているデバイス鍵を用いて、メディア鍵を暗号化して暗号化メディア鍵を生成する。ここで、図４９に示すように、無効化されていないデバイス鍵のうち、最上位のレイヤに存在するノードに割り当てられているデバイス鍵は、ノードＴ７０４に割り当てられたデバイス鍵ＫｅｙＣであるので、鍵管理装置１００は、デバイス鍵ＫｅｙＣを用いて、メディア鍵を暗号化して、暗号化メディア鍵Ｅｉ（ＫｅｙＣ、メディア鍵）を生成し、生成した暗号化メディア鍵Ｅｉ（ＫｅｙＣ、メディア鍵）を、鍵情報記録装置２００を介して、記録媒体に書き込む。

【０２５５】次に、鍵管理装置１００は、上記のデバイス鍵ＫｅｙＣが割り当てられたノードＴ７０４及びノードＴ７０４の下位鍵の全てのノードを除く他のノードについて、これらの他のノードに割り当てられた無効化されていないデバイス鍵のうち、最上位のレイヤに存在するノードに割り当てられているデバイス鍵を用いて、メディア鍵を暗号化して暗号化メディア鍵を生成する。ここで、該当するノードは、ノードＴ７０５であるので、鍵管理装置１００は、ノードＴ７０５に割り当てられたデバイス鍵ＫｅｙＤを用いて、メディア鍵を暗号化して、暗号化メディア鍵Ｅｉ（ＫｅｙＤ、メディア鍵）を生成し、生成した暗号化メディア鍵Ｅｉ（ＫｅｙＤ、メディア鍵）を、鍵情報記録装置２００を介して、記録媒体に書き込む。

【０２５６】次に、鍵管理装置１００は、上記のデバイス鍵ＫｅｙＣが割り当てられたノードＴ７０４及びノードＴ７０４の下位鍵の全てのノード、及び上記のデバイス鍵ＫｅｙＤが割り当てられたノードＴ７０５及びノードＴ７０５の下位鍵の全てのノードを除く他のノードについて、これらの他のノードに割り当てられた無効化されていないデバイス鍵のうち、最上位のレイヤに存在するノードに割り当てられているデバイス鍵を用いて、メ

65　　66

ディア鍵を暗号化して暗号化メディア鍵を生成する。ここで、該当するノードは、ノードＴ７０６であるので、鍵管理装置１００は、ノードＴ７０６に割り当てられたデバイス鍵ＫｅｙＪを用いて、メディア鍵を暗号化して、暗号化メディア鍵Ｅ１（ＫｅｙＪ、メディア鍵）を生成し、生成した暗号化メディア鍵Ｅ１（ＫｅｙＪ、メディア鍵）を、鍵情報記録装置２００を介して、記録媒体に書き込む。

【０２５７】次に、鍵管理装置１００は、上記と同様にして、ノードｔ７０７に割り当てられたデバイス鍵ＫｅｙＫを用いて、メディア鍵を暗号化して、暗号化メディア鍵Ｅ１（ＫｅｙＫ、メディア鍵）を生成し、生成した暗号化メディア鍵Ｅ１（ＫｅｙＫ、メディア鍵）を、鍵情報記録装置２００を介して、記録媒体に書き込む。このようにして、図５０に示す鍵情報Ｄ１０１０が記録媒体に書き込まれる。鍵情報Ｄ１０１０は、この図に示すように、暗号化メディア鍵Ｅ１（ＫｅｙＣ、メディア鍵）、Ｅ１（ＫｅｙＤ、メディア鍵）、Ｅ１（ＫｅｙＪ、メディア鍵）及びＥ１（ＫｅｙＫ、メディア鍵）を、この順序で含んで構成されている。

【０２５８】（記録装置３００ａ）次に、記録装置３００ａが有する特定部３０３により、上記のようにして記録媒体に記憶されたヘッダ情報及び鍵情報から、１個の暗号化メディア鍵を特定する動作について、図５１に示すフローチャートを用いて説明する。特定部３０３は、暗号化メディア鍵の位置を示す変数Ｘ、ユーザ装置自身に関係するＮＲＰの位置を示す変数Ａ、あるレイヤにおけるＮＲＰの数を示す変数Ｗ、及び処理対象となるレイヤ数を示す変数ｉを有している。

【０２５９】特定部３０３は、初期値として、それぞれ変数Ａ＝０、変数Ｗ＝１、変数ｉ＝０とする（ステップＳ３０１）。次に、特定部３０３は、Ａ番目のＮＲＰの下位２ビットのうち、ＩＤ情報の上位ｉビット目の値に対応するビット位置にある値Ｂが「０」であるか、又は「１」であるかをチェックする（ステップＳ３０３）。ここで、対応するビット位置とは、上記の実施の形態においても説明したように、図４に示す木構造において左の経路に「０」、右の経路に「１」が割り当てられ、これらの規則に基づいてＩＤ情報が構成されているので、ＩＤ情報の上位ｉビット目の値「０」は、Ａ番目のＮＲＰの下位２ビットのうちの左ビットに対応し、ｉビット目の値「１」は、Ａ番目のＮＲＰの下位２ビットのうちの右ビットに対応する。

【０２６０】次に、値Ｂ＝０の場合（ステップＳ３０３）、特定部３０３は、先頭のＮＲＰから、最後にチェックしたＮＲＰまでの各ＮＲＰについて、以下の通りチェックする。ただしＡ番目のＮＲＰは含まない。

（ａ）ＮＰＲの最上位ビットが「０」であり、かつ下位２ビットが「１１」でないとき、変数Ｘに「１」を加算する。

【０２６１】（ｂ）ＮＰＲの最上位ビットが「１」であるとき、下位２ビットに含まれる「０」の数を、変数Ｘに加算する。最後にチェックしたＡ番目のＮＲＰについては、ＮＲＰの最上位ビットが「１」であるときのみ、対応するビット位置までの「０」の数を変数Ｘに加算する。ここで、対応するビット自身は含まないものとする。こうして得られた変数Ｘが、暗号化メディア鍵の位置を示している。また、この時点の変数ｉは、デバイス鍵を識別するためのデバイス鍵識別情報である（ステップＳ３０７ｃ）。次に、特定部３０３は、処理を終了する。

【０２６２】一方、値Ｂ＝１の場合（ステップＳ３０３）、さらに、特定部３０３は、ＮＲＰの最上位ビットが「１」でないか否かを判断し、ＮＲＰの最上位ビットが「１」であると判断する場合には（ステップＳ３０８）、このユーザ装置は、無効化されているので、次に、特定部３０３は、処理を終了する。ＮＲＰの最上位ビットが「１」でないと判断する場合に（ステップＳ３０８）、特定部３０３は、レイヤｉに存在するＷ個の全ＮＲＰの下位２ビットに含まれる「１」の数をカウントし、カウントした値を変数Ｗに代入する。ただし、ＮＲＰの最上位ビットが「１」のＮＰＲは、カウントの対象とはしない。こうして得られた変数Ｗが、次のレイヤｉ＋１に存在するＮＲＰの数を示す（ステップＳ３０４ｃ）。

【０２６３】次に、特定部３０３は、レイアｉに存在するＮＲＰのうちの最初のＮＲＰから、対応するビット位置までの各ＮＲＰについて、ＮＲＰの下位２ビットに含まれる「１」の数をカウントし、カウントした値を変数Ａに代入する。ここで、対応するビット位置の値はカウントしない。また、ＮＲＰの最上位ビットが「１」であるＮＲＰは、カウントの対象とはしない。こうして得られた変数Ａが、次のレイヤｉ＋１のＮＲＰのうち、ユーザ装置自身に関係するＮＲＰの位置を示す（ステップＳ３０５ｃ）。

【０２６４】次に、特定部３０３は、変数Ｉ＝ｉ＋１を演算し（ステップＳ３０６）、次にステップＳ３０３へ制御を移し、上述の処理を繰り返す。以上に示すようにして、木構造のリーフからルートへの経路上に存在するデバイス鍵が無効化された場合に限らず、木構造の一部のノードに割り当てられたデバイス鍵が無効化された場合であっても、鍵管理装置によるヘッダ情報及び鍵情報の記録媒体への書込みと、再生装置による暗号化メディア鍵の特定とが行える。

【０２６５】（９）一例として図４に示す木構造を想定し、デバイス鍵が全く漏洩していない初期状態であり、前記木構造には無効化されたノードがないものとする。この場合に、鍵管理装置は、ルートに対応付けられているデバイス鍵ＫｅｙＡを用いて、メディア鍵を暗号化して１個の暗号化メディア鍵を生成する。次に、鍵管理装

置は、前記木構造には無効化されたノードがなく、全てのノードが有効であることを示す特別なＮＲＰ｛００｝を１個生成する。次に、鍵管理装置は、生成した前記暗号化メディア鍵と生成したＮＲＰ｛００｝を、鍵情報記録装置を介して、記録媒体に書き込む。

【０２６６】また、この場合に、再生装置は、前記記録媒体からＮＲＰを読み出し、読み出したＮＲＰが｛００｝のみであり、この他にＮＲＰが前記記録媒体に記録されていないと判断する場合に、再生装置は、木構造において無効化されているノードが全く存在しないものと判断し、次に、前記記録媒体に記録されている前記暗号化メディア鍵を読み出し、再生装置自身が記憶しているデバイス鍵のうち、ルートに対応付けられているデバイス鍵ＫｅｙＡを用いて、読み出した前記暗号化メディア鍵を復号して、メディア鍵を生成する。

【０２６７】また、この場合に、記録装置も、前記再生装置と同様に動作する。

（１０）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【０２６８】また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【０２６９】また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

（１１）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【０２７０】７．まとめ

以上の説明から明らかなように、第１の実施の形態において開示した発明によると、予め記録媒体に記録される鍵情報のヘッダ情報として、ＮＲＰを水準順に並べることにより、鍵情報をコンパクトにでき、プレーヤが効率よく復号すべき暗号化メディア鍵を特定することもできる。

【０２７１】また、第２の実施の形態において開示した発明によると、ヘッダ情報として、あるノードの子孫が全て無効化装置であるか否かを示すビットをＮＲＰの先頭に追加することで、無効化装置が集中した場合にヘッダ情報を少なくすることができる。また、第３の実施の形態において開示した発明によると、ある特定のパターンで、あるノードの子孫が全て無効化装置であるか否かを判断することで、さらにヘッダ情報を少なく抑えることができる。

【０２７２】また、第４の実施の形態及び第５の実施の形態において開示した発明によると、ＮＲＰの順序を、第１～第３の実施の形態において開示した順序以外のものとすることができる。

８．産業上の利用の可能性

上記において説明した鍵管理装置及び利用者装置から構成される著作物保護システムは、音楽、映画、小説などのデジタル化された著作物をＤＶＤなどの記録媒体に格納して市場を流通させる場合において、コンテンツの不正な使用を防ぐための仕組みとして好適である。

【０２７３】

【発明の効果】上記目的を達成するために本発明は、ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置と、１以上の利用者装置とからなる著作物保護システムであって、前記鍵管理装置は、デバイス鍵を各利用者装置に割り当て、各利用者装置は、割り当てられたデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号し、前記鍵管理装置は、ｎ分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を配慮しているデバイス鍵記憶手段と、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段とを備え、前記利用者装置は、前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディ

ア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段とを備える。

【０２７４】この構成によると、鍵管理装置は、複数の暗号化メディア鍵及び複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、利用者装置は、前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から暗号化メディア鍵を特定するので、利用者装置は、自らに割り当てられた暗号化メディア鍵を効率良く決定することができる。

【０２７５】また、本発明は、ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当てる鍵管理装置であって、ｎ分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段とを備える。また、ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１個以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置であって、前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段とを備える。

【０２７６】この構成によると、鍵管理装置は、複数の暗号化メディア鍵及び複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、利用者装置は、前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から暗号化メディア鍵を特定するので、利用者装置は、自らに割り当てられた暗号化メディア鍵を効率良く決定することができる。

【０２７７】ここで、前記ｎ分木は、複数のレイヤから構成され、前記鍵情報生成手段は、得られた複数の暗号化メディア鍵を、ルートを起点とし、ルート側のレイヤからリーフ側のレイヤの順序である前記配列順序に従って記録媒体に書き込み、前記無効化情報生成手段は、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む。また、前記ｎ分木は、複数のレイヤから構成され、前記複数の暗号化メディア鍵は、ルートを起点とし、ルート側のレイヤからリーフ側のレイヤへの順序である前記配列順序に従って記録媒体に書き込まれ、前記複数の無効化情報は、前記配列順序に従って前記記録媒体に書き込まれ、前記特定手段は、前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、前記暗号化メディア鍵を特定する。

【０２７８】この構成によると、前記配列順序は、ルートを起点とし、ルート側のレイヤからリーフ側のレイヤへの順序であるので、鍵管理装置及び利用者装置において前記配列順序を確実に決定することができる。ここ

で、前記鍵情報生成手段は、得られた複数の暗号化メディア鍵を、ルートを起点とし、ルートから各リーフへ至る経路上に配されるノードの順序であって、重複して配列されない前記配列順序に従って記録媒体に書き込み、前記無効化情報生成手段は、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む。また、前記複数の暗号化メディア鍵は、ルートを起点とし、ルートから各リーフへ至る経路上に配されるノードの順序であって、重複して配列されない前記配列順序に従って記録媒体に書き込まれ、前記複数の無効化情報は、前記配列順序に従って前記記録媒体に書き込まれ、前記特定手段は、前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、前記暗号化メディア鍵を特定する。

【０２７９】この構成によると、前記配列順序は、ルートを起点とし、重複して配列されないように、ルートから各リーフへ至る経路上に配されるノードの順序であるので、鍵管理装置及び利用者装置において前記配列順序を確実に決定することができる。ここで、前記無効化情報生成手段は、リーフを除き、無効化された全てのノードについて、無効化情報を生成する。また、リーフを除き、無効化された全てのノードについて、無効化情報が生成されて、前記記録媒体に書き込まれ、前記特定手段は、前記複数の無効化情報を用いて、前記暗号化メディア鍵を特定する。

【０２８０】この構成によると、無効化された全てのノードについて、無効化情報を生成するので、鍵管理装置及び利用者装置において無効化されたノードを確実に決定することができる。ここで、前記無効化情報生成手段は、リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す特別無効化情報を生成し、前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成を抑制し、リーフを除く他の無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成する。また、リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す特別無効化情報が生成されて前記記録媒体に書き込まれ、前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成が抑制され、リーフを除く他の無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報が生成されて前記記録媒体に書き込まれ、前記特定手段は、前記特別無効化情報及び前記無効化情報を用いて、前記暗号化メディア鍵を特定する。

【０２８１】この構成によると、下位側に接続する全てのノードが無効化されていることを示す特別な無効化情報を生成するので、下位側に接続する全てのノードが無効化されているものが多い場合に、記録媒体の容量を節約することができる。

【図面の簡単な説明】

【図１】著作物保護システム１０の構成を示すブロック図である。

【図２】鍵管理装置１００の構成を示すブロック図である。

【図３】木構造テーブルＤ１００のデータ構造の一例を示す。

【図４】木構造Ｔ１００を示す概念図である。

【図５】無効化されたノードを含む木構造Ｔ２００を示す概念図である。

【図６】ノード無効化パターンの一例を示すデータ構造図である。

【図７】複数個の暗号化メディア鍵を含む鍵情報の一例を示すデータ構造図である。

【図８】記録装置３００ａの構成を示すブロック図である。

【図９】再生装置４００ａの構成を示すブロック図である。

【図１０】ユーザ装置へデバイス鍵を割り当てる動作、鍵情報の生成と記録媒体への書き込みの動作及びユーザ装置によるコンテンツの暗号化又は復号の動作を示すフローチャートである。特に、デバイス鍵が特に、デバイス鍵が不正な第三者により暴露されるまでの、各装置の動作を示すフローチャートである。

【図１１】デバイス鍵が不正な第三者により暴露された後における、暴露されたデバイス鍵に対応する木構造の内のノードの無効化の動作、新たな鍵情報の生成と記録媒体への書込みの動作、及びユーザ装置によるコンテンツの暗号化又は復号の動作を示すフローチャートである。

【図１２】木構造構築部１０１による木構造テーブルの生成と木構造格納部１０２への木構造テーブルの書き込みの動作を示すフローチャートである。

【図１３】デバイス鍵割当部１０３によるデバイス鍵とＩＤ情報とを各ユーザ装置へ出力する動作を示すフローチャートである。

【図１４】木構造更新部１０５による木構造の更新の動作を示すフローチャートである。

【図１５】鍵情報ヘッダ生成部１０６によるヘッダ情報の生成の動作を示すフローチャートである。

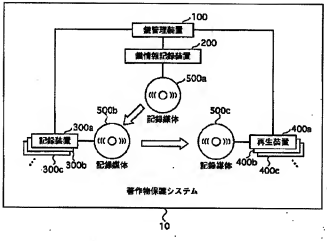
【図１６】鍵情報生成部１０７による鍵情報の生成の動作を示すフローチャートである。

【図１７】記録装置３００ａが有する特定部３０３により、記録媒体５００ｂに記憶されている鍵情報から、１個の暗号化メディア鍵を特定する動作を示すフローチャートである。

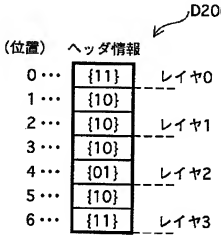
【図１８】第１の実施の形態において、一例として無効化されるユーザ装置が木構造の中で特定のリーフに集中して発生する可能性がある場合の木構造の一例を示す。
【図１９】第２の実施の形態において、無効化されるユーザ装置が木構造の中で特定のリーフに集中して発生した場合における特別なノード無効化パターンを示す木構造である。
【図２０】木構造テーブルＤ４００のデータ構造の一例を示す。
【図２１】ヘッダ情報Ｄ５００のデータ構造の一例を示す。
【図２２】鍵情報Ｄ６００のデータ構造の一例を示す。
【図２３】鍵情報ヘッダ生成部１０６によるヘッダ情報の生成の動作を示すフローチャートである。図２４へ続く。
【図２４】鍵情報ヘッダ生成部１０６によるヘッダ情報の生成の動作を示すフローチャートである。図２５へ続く。
【図２５】鍵情報ヘッダ生成部１０６によるヘッダ情報の生成の動作を示すフローチャートである。図２６へ続く。
【図２６】鍵情報ヘッダ生成部１０６によるヘッダ情報の生成の動作を示すフローチャートである。図２５から続く。
【図２７】記録装置３００ａが有する特定部３０３により、記録媒体５００ｂに記憶されている鍵情報から、１個の暗号化メディア鍵を特定する動作を示すフローチャートである。
【図２８】第３の実施の形態において、特別なノード無効化パターンを示す木構造である。
【図２９】ヘッダ情報Ｄ７００のデータ構造の一例を示す。
【図３０】鍵情報Ｄ８００のデータ構造の一例を示す。
【図３１】ヘッダ情報の生成の動作を示すフローチャートである。図３２へ続く。
【図３２】ヘッダ情報の生成の動作を示すフローチャートである。図３３へ続く。
【図３３】ヘッダ情報の生成の動作を示すフローチャートである。図３４へ続く。
【図３４】ヘッダ情報の生成の動作を示すフローチャートである。図３３から続く。
【図３５】記録装置３００ａが有する特定部３０３により、記録媒体５００ｂに記憶されている鍵情報から、１個の暗号化メディア鍵を特定する動作を示すフローチャートである。
【図３６】第４の実施の形態における複数のノード無効化パターンの並べ方を示す木構造である。
【図３７】木構造テーブルＤ１００のデータ構造の一例を示す。
【図３８】ヘッダ情報Ｄ９００のデータ構造の一例を示す。
【図３９】木構造構築部１０１による木構造テーブルの生成と木構造格納部１０２への木構造テーブルの書き込みの動作を示すフローチャートである。
【図４０】鍵情報ヘッダ生成部１０６によるヘッダ情報の生成の動作を示すフローチャートである。図４１へ続く。
【図４１】鍵情報ヘッダ生成部１０６によるヘッダ情報の生成の動作を示すフローチャートである。図４０から続く。
【図４２】記録装置３００ａが有する特定部３０３により、記録媒体５００ｂに記憶されている鍵情報から、１個の暗号化メディア鍵を特定する動作を示すフローチャートである。
【図４３】鍵情報ヘッダ生成部１０６によるヘッダ情報の生成の動作を示すフローチャートである。図４４へ続く。
【図４４】鍵情報ヘッダ生成部１０６によるヘッダ情報の生成の動作を示すフローチャートである。図４５へ続く。
【図４５】鍵情報ヘッダ生成部１０６によるヘッダ情報の生成の動作を示すフローチャートである。図４６へ続く。
【図４６】鍵情報ヘッダ生成部１０６によるヘッダ情報の生成の動作を示すフローチャートである。図４５から続く。
【図４７】記録装置３００ａが有する特定部３０３により、記録媒体５００ｂに記憶されている鍵情報から、１個の暗号化メディア鍵を特定する動作を示すフローチャートである。
【図４８】著作物保護システム１０ｆの構成を示すブロック図である。
【図４９】無効化されたデバイス鍵ＫｅｙＡ、ＫｅｙＢ及びＫｅｙＥが割り当てられたノードを含む木構造Ｔ７００を示す概念図である。
【図５０】ヘッダ情報Ｄ１０００及び鍵情報Ｄ１０１０の構成を示すデータ構造図である。
【図５１】記録装置３００ａが有する特定部３０３により、１個の暗号化メディア鍵を特定する動作を示すフローチャートである。
【符号の説明】
１０、１０ｂ～１０ｆ　著作物保護システム
１００　鍵管理装置
１００ｄ　鍵管理装置
１０１　木構造構築部
１０２　木構造格納部
１０３　デバイス鍵割当部
１０４　無効化装置指定部
１０５　木構造更新部
１０６　鍵情報ヘッダ生成部

１０７　鍵情報生成部
２００　鍵情報記録装置
３００ａ、３００ｂ、３００ｃ　記録装置
３０１　鍵情報記憶部
３０２　復号部
３０３　特定部
３０４　暗号部
３０５　コンテンツ記憶部
４００ａ、４００ｂ、４００ｃ　再生装置
＊４０１　鍵情報記憶部
４０２　特定部
４０３　復号部
４０４　復号部
４０５　再生部
５００ａ、５００ｂ、５００ｃ、５００ｄ　記録媒体
１７０１　データ記録装置
１７０３ａ、１７０３ｂ、１７０３ｃ　データ再生装置
＊

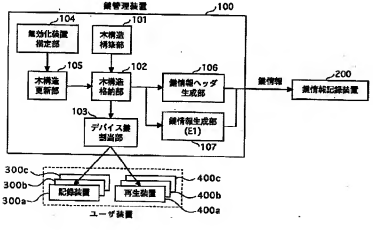
【図１】



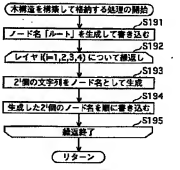
【図６】



【図２】



【図１２】

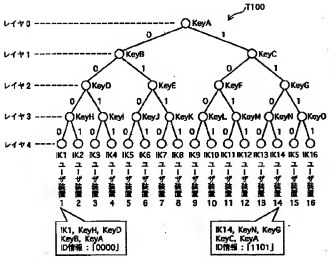


【図３】

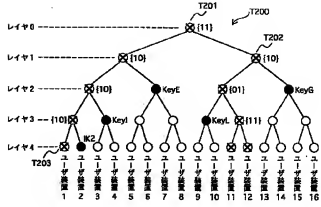
木構造テーブル　D100

ノード情報		
ノード名	デバイス鍵	無効化フラグ
ルート	KeyA	1
0	KeyB	1
1	KeyC	1
00	KeyD	1
01	KeyE	0
10	KeyF	1
11	KeyG	0
000	KeyH	1
001	KeyI	0
010	KeyJ	0
⋮	⋮	⋮
111	KeyO	0
0000	IK1	1
0001	IK2	0
0010	IK3	0
0011	IK4	0
⋮	⋮	⋮
1111	IK16	0

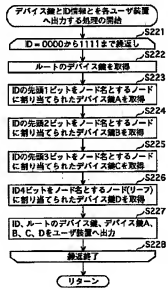
【図４】



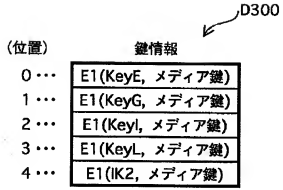
【図５】



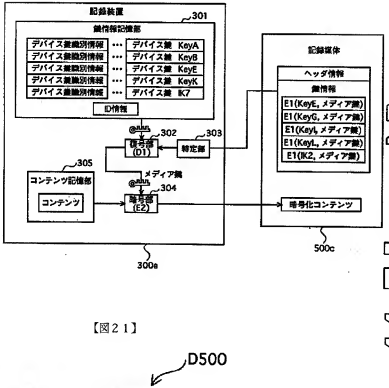
【図１３】



【図７】

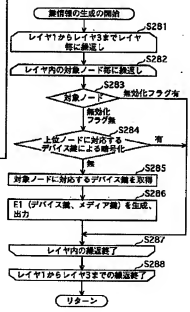


【図８】

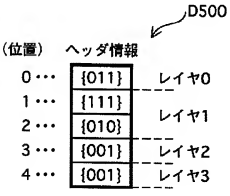


【図１４】

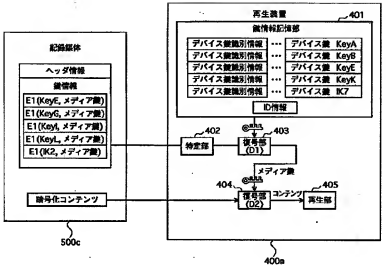
【図１６】



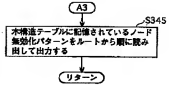
【図２１】



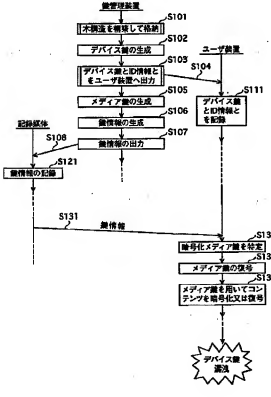
【図９】



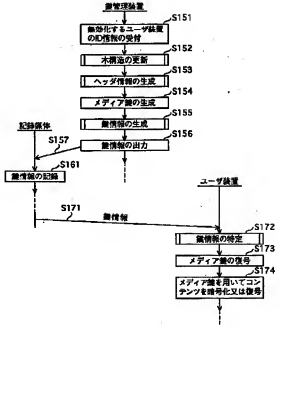
【図２６】



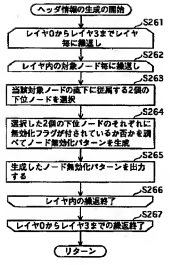
【図１０】



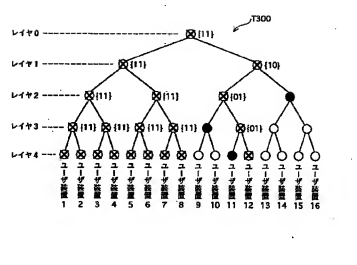
【図１１】



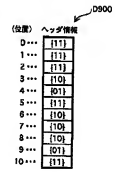
【図１５】



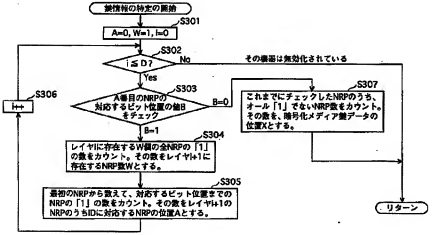
【図１８】



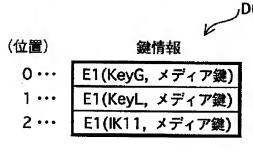
【図３８】



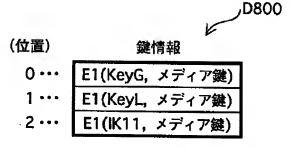
【図１７】



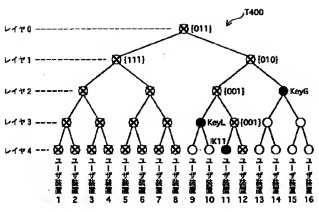
【図２２】



【図３０】



【図１９】

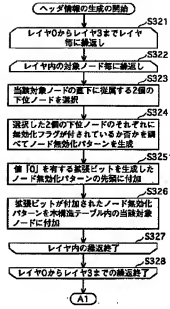


【図２０】

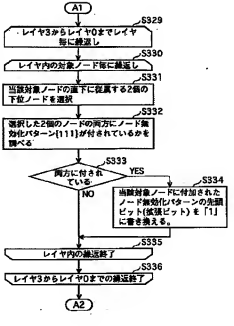
木構造テーブル D400

ノード名	デバイス鍵	無効化フラグ	ノード無効化パターン
ルート	KeyA	1	{011}
0	KeyB	1	{111}
1	KeyC	1	{010}
00	KeyD	1	~~{111}~~
01	KeyE	1	~~{111}~~
10	KeyF	1	{001}
11	KeyG	0	
000	KeyH	1	~~{111}~~
001	KeyI	1	~~{111}~~
010	KeyJ	1	~~{111}~~
⋮	⋮	⋮	
111	KeyO	0	
0000	IK1	1	~~{111}~~
0001	IK2	1	~~{111}~~
0010	IK3	1	~~{111}~~
0011	IK4	1	~~{111}~~
⋮	⋮	⋮	
1111	IK16	0	

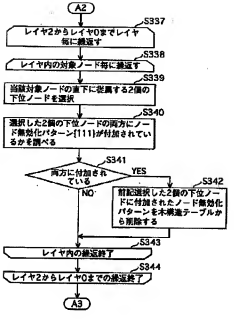
【図２３】



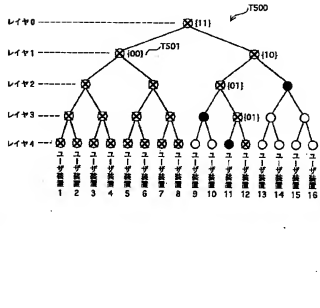
【図２４】



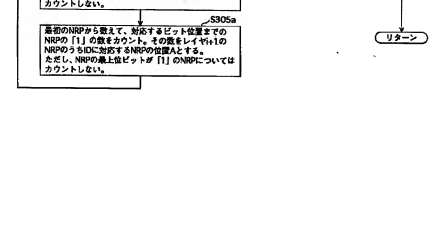
【図２５】


A2
S337
レイヤ2からレイヤ0までレイヤ毎に繰返す
S338
レイヤ内の対象ノード毎に繰返す
S339
当該対象ノードの直下に従属する2個の下位ノードを選択
S340
選択した2個の下位ノードの両方ノードに無効化パターン[111]が付加されているかを調べる
S341
両方に付加されている
YES
NO
S342
前記選択した2個の下位ノードに付加されたノード無効化パターンを木構造テーブルから削除する
S343
レイヤ内の繰返終了
S344
レイヤ2からレイヤ0までの繰返終了
A3

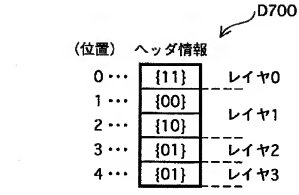
【図２８】


T500
レイヤ0
[11]
T501
レイヤ1
[00]
[10]
レイヤ2
[01]
レイヤ3
[01]
レイヤ4
ユーザ装置1
ユーザ装置2
ユーザ装置3
ユーザ装置4
ユーザ装置5
ユーザ装置6
ユーザ装置7
ユーザ装置8
ユーザ装置9
ユーザ装置10
ユーザ装置11
ユーザ装置12
ユーザ装置13
ユーザ装置14
ユーザ装置15
ユーザ装置16

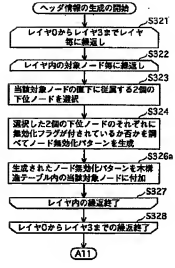
【図２７】


最情報の特定の開始
S301
A=0, W=1, I=0
S302
I≦D?
No
Yes
その機器は無効化されている
S303
I番目のNRPの対応するビット位置の値をチェック
S306
I++
B=0
B=1
S307a
これまでにチェックしたNRPのうち、下位2ビットがオール「1」でないNRP数をカウント。その数を、当今化メディア層データの位置Aとする。
S304a
レイヤiに存在するW個のNRPの「1」の数をカウント。その数をレイヤi+1に存在するNRP数Wとする。ただし、NRPの最上位ビットが「1」のNRPについてはカウントしない。
S305a
最初のNRPから数えて、対応するビット位置までのNRPの「1」の数をカウント。その数をレイヤi+1のNRPのうちIDに対応するNRPの位置Aとする。ただし、NRPの最上位ビットが「1」のNRPについてはカウントしない。
リターン

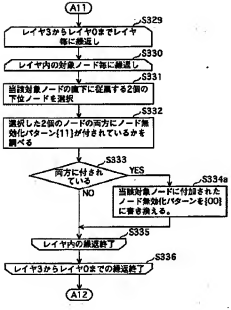
【図２９】



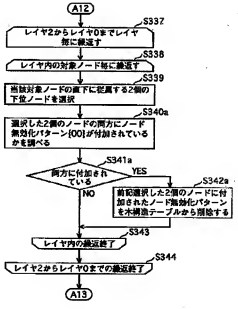
【図３１】



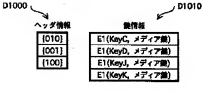
【図３２】



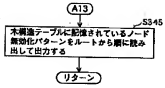
【図３３】



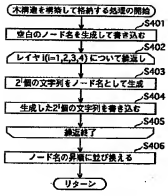
【図５０】



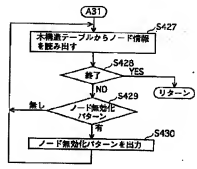
【図３４】



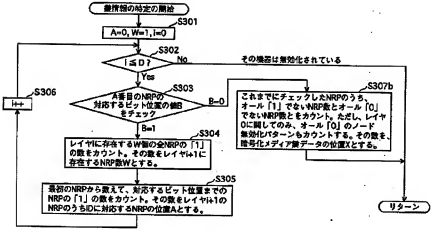
【図３９】



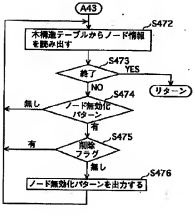
【図４１】



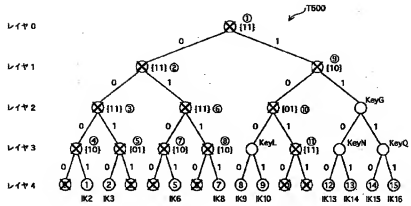
【図３５】



【図４６】



【図３６】



【図３７】

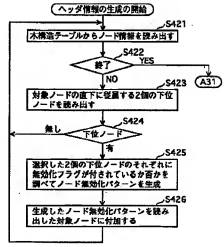
D1000

木構造テーブル

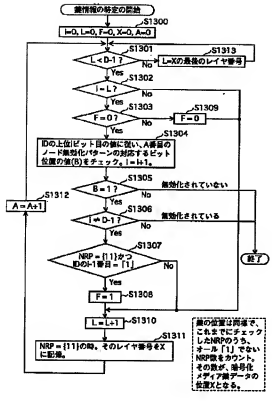
ノード情報		
ノード名	デバイス鍵	無効化フラグ
(空白)	KeyA	
0	KeyB	
00	KeyD	
000	KeyH	
0000	IK1	
0001	IK2	
001	KeyI	
0010	IK3	
0011	IK4	
01	KeyE	
010	KeyJ	
0100	IK5	
0101	IK6	
011	KeyK	
0110	IK7	
0111	IK8	

ノード情報		
ノード名	デバイス鍵	無効化フラグ
1	KeyC	
10	KeyF	
100	KeyL	
1000	IK9	
1001	IK10	
101	KeyM	
1010	IK11	
1011	IK12	
11	KeyG	
110	KeyN	
1100	IK13	
1101	IK14	
111	KeyO	
1110	IK15	
1111	IK16	

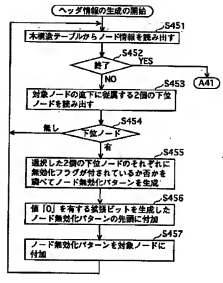
【図４０】



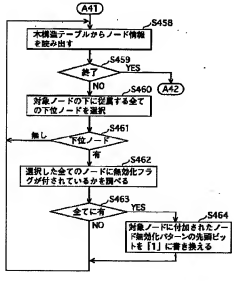
【図４２】



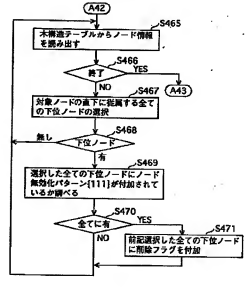
【図４３】



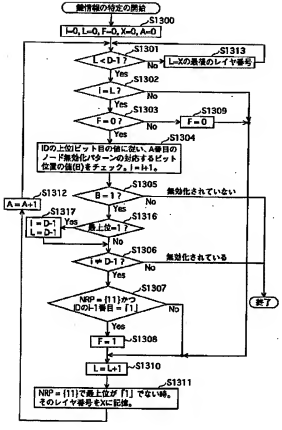
【図４４】



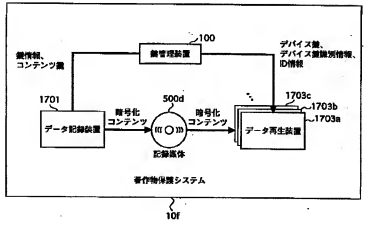
【図４５】



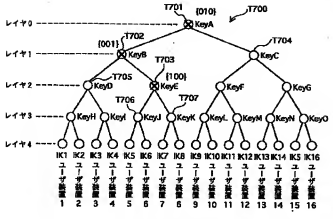
【図４７】


鍵情報の特定の開始
S1300
I=0, L=0, F=0, X=0, A=0
S1301
L < D-1 ?
No
S1313
L=Xの最後のレイヤ番号
Yes
S1302
I = L ?
No
Yes
S1303
F = 0 ?
No
S1309
F = 0
Yes
S1304
IDの上位ビット目の値に従い、A番目のノード無効化パターンの対応するビット位置の値(B)をチェック。I = I+1。
S1305
B = 1 ?
No
無効化されていない
Yes
S1312
A = A+1
S1316
最上位=1 ?
Yes
S1317
I = D-1
L = D-1
No
S1306
I = D-1 ?
No
無効化されている
Yes
S1307
NRP = {1}かつ
上位I-1番目 = {1}
No
終了
Yes
S1308
F = 1
S1310
L = L+1
S1311
NRP = {1}で最上位が「1」でない時。
そのレイヤ番号をXに記憶。

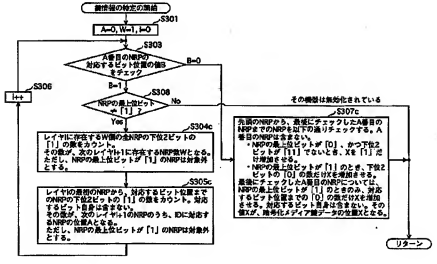
【図４８】


100
鍵管理装置
鍵情報、
コンテンツ鍵
デバイス鍵、
デバイス識別情報、
ID情報
1701
500d
1703c
1703b
1703a
暗号化
コンテンツ
暗号化
コンテンツ
データ記録装置
データ再生装置
記録媒体
著作物保護システム
10f

【図４９】



【図５１】



フロントページの続き

(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Ｆターム(参考)　5J104 AA16 EA09 EA17 PA14

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成16年7月8日(2004.7.8)

【公開番号】特開2003-204320(P2003-204320A)
【公開日】平成15年7月18日(2003.7.18)
【出願番号】特願2002-303509(P2002-303509)
【国際特許分類第７版】
　Ｈ０４Ｌ　 9/08
【ＦＩ】
　Ｈ０４Ｌ　 9/00　　６０１Ｂ
　Ｈ０４Ｌ　 9/00　　６０１Ａ

【手続補正書】
【提出日】平成15年6月2日(2003.6.2)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置と、１以上の利用者装置とからなる著作物保護システムであって、前記鍵管理装置は、デバイス鍵を各利用者装置に割り当て、各利用者装置は、割り当てられたデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号し、
前記鍵管理装置は、
ｎ分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、
複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、
リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段とを備え、
前記利用者装置は、
前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、
特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、
生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段と

を備えることを特徴とする著作物保護システム。
【請求項２】
ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当てる鍵管理装置であって、
ｎ分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、
複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、
リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段と
を備えることを特徴とする鍵管理装置。
【請求項３】
前記ｎ分木は、複数のレイヤから構成され、
前記鍵情報生成手段は、得られた複数の暗号化メディア鍵を、ルートを起点とし、ルート側のレイヤからリーフ側のレイヤへの順序である前記配列順序に従って記録媒体に書き込み、
前記無効化情報生成手段は、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む
ことを特徴とする請求項２に記載の鍵管理装置。
【請求項４】
前記鍵情報生成手段は、得られた複数の暗号化メディア鍵を、ルートを起点とし、ルートから各リーフへ至る経路上に配されるノードの順序であって、重複して配列されない前記配列順序に従って記録媒体に書き込み、
前記無効化情報生成手段は、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む
ことを特徴とする請求項２に記載の鍵管理装置。
【請求項５】
前記無効化情報生成手段は、リーフを除き、無効化された全てのノードについて、無効化情報を生成する
ことを特徴とする請求項２に記載の鍵管理装置。
【請求項６】
前記無効化情報生成手段は、
リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す特別無効化情報を生成し、
前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成を抑制し、
リーフを除く他の無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成する
ことを特徴とする請求項２に記載の鍵管理装置。
【請求項７】
前記無効化情報生成手段は、
リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す第１付加情報と、下位のｎ個のノードのそれぞれが無効化されていることを示すｎ桁の情報と

から構成される特別無効化情報を生成し、
前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成を抑制し、
リーフを除く他の無効化されたノードについて、下位側に接続する全てのノードが無効化されていない旨を示す第２付加情報と、下位のｎ個のノードのそれぞれが無効化されているか否かを示すｎ桁の情報とから構成される無効化情報を生成する
ことを特徴とする請求項６に記載の鍵管理装置。
【請求項８】
前記無効化情報生成手段は、
リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位のｎ個のノードのそれぞれが無効化されていることを示すｎ桁の特別値から構成される特別無効化情報を生成し、
前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成を抑制し、
リーフを除く他の無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示すｎ桁の無効化情報を生成する
ことを特徴とする請求項６に記載の鍵管理装置。
【請求項９】
ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当てる鍵管理装置であって、
ｎ分木において一部のノードは、無効化されており、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、
複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、
リーフを除き、無効化された各ノードについて、
下位のｎ個のノードの少なくとも１個が無効化されている場合に、それぞれが無効化されているか否かを示す第１無効化情報を生成し、
下位のｎ個のノードのいずれも無効化されていない場合に、いずれのノードも無効化されていないことを示す第２無効化情報を生成し、
その結果、１個以上の第１無効化情報、１個以上の第２無効化情報、又は１個以上の第１無効化情報及び１個以上の第２無効化情報が得られ、
得られた１個以上の第１無効化情報、１個以上の第２無効化情報、又は１個以上の第１無効化情報及び１個以上の第２無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段と
を備えることを特徴とする鍵管理装置。
【請求項１０】
ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当てる鍵管理装置であって、ｎ分木を構成する全てのノードは、有効であり、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、
各利用者装置に共通に割り当てられた１個のデバイス鍵に基づいて、１個のメディア鍵を暗号化して１個の暗号化メディア鍵を生成し、生成した前記暗号化メディア鍵を、記録媒体に書き込む鍵情報生成手段と、
ｎ分木を構成する全てのノードが有効であることを示す情報を前記記録媒体に書き込む無効化情報生成手段と
を備えることを特徴とする鍵管理装置。
【請求項１１】
ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１個以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の１個

のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置であって、
前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、
前記利用者装置は、
前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、
特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、
生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段と
を備えることを特徴とする利用者装置。
【請求項１２】
前記ｎ分木は、複数のレイヤから構成され、
前記複数の暗号化メディア鍵は、ルートを起点とし、ルート側のレイヤからリーフ側のレイヤへの順序である前記配列順序に従って記録媒体に書き込まれ、
前記複数の無効化情報は、前記配列順序に従って前記記録媒体に書き込まれ、前記特定手段は、前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、前記暗号化メディア鍵を特定する
ことを特徴とする請求項１１に記載の利用者装置。
【請求項１３】
前記複数の暗号化メディア鍵は、ルートを起点とし、ルートから各リーフへ至る経路上に配されるノードの順序であって、重複して配列されない前記配列順序に従って記録媒体に書き込まれ、
前記複数の無効化情報は、前記配列順序に従って前記記録媒体に書き込まれ、前記特定手段は、前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、前記暗号化メディア鍵を特定する
ことを特徴とする請求項１１に記載の利用者装置。
【請求項１４】
リーフを除き、無効化された全てのノードについて、無効化情報が生成されて、前記記録媒体に書き込まれ、
前記特定手段は、前記複数の無効化情報を用いて、前記暗号化メディア鍵を特定する
ことを特徴とする請求項１１に記載の利用者装置。
【請求項１５】
リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す特別無効化情報が生成されて前記記録媒体に書き込まれ、

前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成が抑制され、
リーフを除く他の無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報が生成されて前記記録媒体に書き込まれ、
前記特定手段は、前記特別無効化情報及び前記無効化情報を用いて、前記暗号化メディア鍵を特定する
ことを特徴とする請求項１１に記載の利用者装置。
【請求項１６】
リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す第１付加情報と、下位のｎ個のノードのそれぞれが無効化されていることを示すｎ桁の情報とから構成される特別無効化情報が生成されて前記記録媒体に書き込まれ、
前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成が抑制され、
リーフを除く他の無効化されたノードについて、下位側に接続する全てのノードが無効化されていない旨を示す第２付加情報と、下位のｎ個のノードのそれぞれが無効化されているか否かを示すｎ桁の情報とから構成される無効化情報が生成されて前記記録媒体に書き込まれ、
前記特定手段は、前記特別無効化情報及び前記無効化情報を用いて、前記暗号化メディア鍵を特定する
ことを特徴とする請求項１５に記載の利用者装置。
【請求項１７】
リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位のｎ個のノードのそれぞれが無効化されていることを示すｎ桁の特別値から構成される特別無効化情報が生成されて前記記録媒体に書き込まれ、
前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成が抑制され、
リーフを除く他の無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示すｎ桁の無効化情報が生成されて前記記録媒体に書き込まれ、
前記特定手段は、前記特別無効化情報及び前記無効化情報を用いて、前記暗号化メディア鍵を特定する
ことを特徴とする請求項１５に記載の利用者装置。
【請求項１８】
ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１個以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置であって、
前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、一部のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化された各ノードについて、下位のｎ個のノードの少なくとも１個が無効化されている場合に、それぞれが無効化されているか否かを示す第１無効化情報を生成し、下位のｎ個のノードのいずれも無効化されていない場合に、いずれのノードも無効化されていないことを示す第２無効化情報を生成し、その結果、１個以上の第１無効化情報、１個以上の第２無効化情報、又は１個以上の第１無効化情報及び１個以上の第２無効化情報が得られ、得られた１個以上の第１無効化情報、１個以上の第２無効化情報、又は１個以上の第１無効化情報及び１個以上の第２無効化情報を

、前記配列順序に従って前記記録媒体に書き込み、
前記利用者装置は、
前記記録媒体に前記配列順序に従って書き込まれた前記第１無効化情報、前記第２無効化情報、又は前記第１無効化情報及び前記第２無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、
特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、
生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段と
を備えることを特徴とする利用者装置。
【請求項１９】
ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１個以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置であって、
前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ｎ分木を構成する全てのノードは、有効であり、各利用者装置に共通に割り当てられた１個のデバイス鍵に基づいて、１個のメディア鍵を暗号化して１個の暗号化メディア鍵を生成し、生成した前記暗号化メディア鍵を、記録媒体に書き込み、ｎ分木を構成する全てのノードが有効であることを示す情報を前記記録媒体に書き込み、
前記利用者装置は、
前記記録媒体に有効であることを示す前記情報が記録されていると判断する場合に、前記記録媒体に記録されている前記暗号化メディア鍵を読み出す読出手段と、
読み出した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、
生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段と
を備えることを特徴とする利用者装置。
【請求項２０】
ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置で用いられる鍵管理プログラムであって、前記鍵管理装置は、ｎ分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、前記デバイス鍵を各利用者装置に割り当て、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段を備え、
前記鍵管理プログラムは、
複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成ステップと、
リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成ステップと
を含むことを特徴とする鍵管理プログラム。
【請求項２１】

ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置で用いられる利用者プログラムであって、

前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、

前記利用者プログラムは、

前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定ステップと、

特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号ステップと、

生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号ステップと

を含むことを特徴とする利用者プログラム。

【請求項２２】

ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置で用いられる鍵管理方法であって、前記鍵管理装置は、ｎ分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、前記デバイス鍵を各利用者装置に割り当て、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段を備え、

前記鍵管理方法は、

無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵をそれぞれ用いて、１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成ステップと、

リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成ステップと

を含むことを特徴とする鍵管理方法。

【請求項２３】

ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１以上のデバイス鍵が割り当てられ、割り当てられた複数のデバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置で用いられる利用方法であって、

前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノード

は、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、
前記利用方法は、
前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定ステップと、
特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号ステップと、
生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号ステップと
を含むことを特徴とする利用方法。

【請求項２４】

ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置で用いられる鍵管理プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、前記鍵管理装置は、ｎ分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、前記デバイス鍵を各利用者装置に割り当て、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段を備え、
前記鍵管理プログラムは、
複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成ステップと、
リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成ステップと
を含むことを特徴とする記録媒体。

【請求項２５】

ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１以上のデバイス鍵が割り当てられ、割り当てられた複数のデバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置で用いられる利用者プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、
前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き

、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、
前記利用者プログラムは、
前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定ステップと、
特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号ステップと、
生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号ステップと
を含むことを特徴とする記録媒体。
【請求項２６】
コンピュータ読み取り可能な記録媒体であって、
ｎ分木（ｎは、２以上の整数）の構成に係る配列順序に従って、複数の暗号化メディア鍵及び複数の無効化情報を記録しており、
ここで、前記複数の暗号化メディア鍵及び前記複数の無効化情報は、鍵管理装置により生成され、記録され、前記鍵管理装置は、ｎ分木に関連付けて１個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当て、
前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む
ことを特徴とする記録媒体。
【請求項２７】
対象物の無効化を管理する無効化管理装置と対象物が無効か否かを判定する無効判定装置とから構成される認証システムであって、
前記無効化管理装置は、
木構造の複数のリーフが、それぞれ複数の対象物に対応し、各リーフを示すリーフ識別子は、各対象物を識別し、前記対象物のうち少なくとも１個の対象物が無効化されており、無効化された対象物を識別するリーフ識別子により示されるリーフからルートに至るまでの全てのノードは無効化されており、前記木構造を構成する複数のノードを有する木構造記憶手段と、
リーフを除く無効化された各ノードについて、下位のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記木構造の構成に係る配列順序に従って配列して無効化リストを生成する無効化リスト生成手段と、
生成した無効化リストを出力する出力手段とを含み、
前記無効判定装置は、
前記木構造の１個のリーフを示すリーフ識別子であり、対象物を識別する識別子を取得する識別子取得手段と、
前記無効化リストを取得するリスト取得手段と、

取得した前記無効化リスト内に配列されている前記無効化情報を用いて、ルートから前記リーフに至る経路の構築を試み、構築された経路内に前記リーフが含まれる場合に、前記対象物が無効であると判断し、前記リーフが含まれない場合に、前記対象物が有効であると判断する判定手段と、
前記対象物が無効であると判断される場合に、前記対象物の利用を禁止し、前記対象物が有効であると判断される場合に、前記対象物を利用する利用手段とを含む
ことを特徴とする認証システム。
【請求項２８】
対象物の無効化を管理する無効化管理装置であって、
木構造の複数のリーフが、それぞれ複数の対象物に対応し、各リーフを示すリーフ識別子は、各対象物を識別し、前記対象物のうち少なくとも１個の対象物が無効化されており、無効化された対象物を識別するリーフ識別子により示されるリーフからルートに至るまでの全てのノードは無効化されており、前記木構造を構成する複数のノードを有する木構造記憶手段と、
リーフを除く無効化された各ノードについて、下位のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記木構造の構成に係る配列順序に従って配列して無効化リストを生成する無効化リスト生成手段と、
生成した無効化リストを出力する出力手段と
を備えることを特徴とする無効化管理装置。
【請求項２９】
対象物が無効か否かを判定する無効判定装置であって、
無効化管理装置は、木構造を構成する複数のノードを有し、前記木構造の複数のリーフは、それぞれ複数の対象物に対応し、各リーフを示すリーフ識別子は、各対象物を識別し、前記対象物のうち少なくとも１個の対象物が無効化されており、無効化された対象物を識別するリーフ識別子により示されるリーフからルートに至るまでの全てのノードは無効化されており、リーフを除く無効化された各ノードについて、下位のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記木構造の構成に係る配列順序に従って配列して無効化リストを生成し、生成した無効化リストを出力し、
前記無効判定装置は、
前記木構造の１個のリーフを示すリーフ識別子であり、対象物を識別する識別子を取得する識別子取得手段と、
前記無効化管理装置から前記無効化リストを取得するリスト取得手段と、
取得した前記無効化リスト内に配列されている前記無効化情報を用いて、ルートから前記リーフに至る経路の構築を試み、構築された経路内に前記リーフが含まれる場合に、前記対象物が無効であると判断し、前記リーフが含まれない場合に、前記対象物が有効であると判断する判定手段と、
前記対象物が無効であると判断される場合に、前記対象物の利用を禁止し、前記対象物が有効であると判断される場合に、前記対象物を利用する利用手段と
を備えることを特徴とする無効判定装置。
【請求項３０】
対象物の無効化に係る無効化リストを記録しているコンピュータ読取り可能な記録媒体であって、
無効化管理装置は、
木構造の複数のリーフが、それぞれ複数の対象物に対応し、各リーフを示すリーフ識別子は、各対象物を識別し、前記対象物のうちいずれも無効化されておらず、全てのノードは、無効化されておらず、前記木構造を構成する複数のノードを有する木構造記憶手段と、
木構造を構成する全てのノードは、無効化されていないと判断し、無効化された対象物が存在しないことを示す無効化リストを生成する無効化リスト生成手段とを含み、

前記記録媒体は、生成された前記無効化リストを記録している
ことを特徴とする記録媒体。